Just Enough “Security” Camera Retention Curiosities Anthology

Just Enough “Security” Camera Retention Curiosities Anthology

Who is keeping it, what are they doing with it and what do you have to say about it?

Cameras, cameras everywhere! Where do you suppose all those pictures come from and just where do they go? Who gets to watch and listen? Good luck finding out. Seems like everybody could be in the loop including your next door neighbor. ChatGPT.com can do an amazing research job if your curiosity peaks around one special area. The site often suggests additional avenues at the end of an answer. Remember, if there is a camera, there is probably a built-in microphone with it to give context. Can you walk into a bank or store, or down a street or get in your own car without someone you don’t know going click, click, click and doing anything they like with what they get without saying boo to you about your personal information? Here are some probing questions and answers with several short bibliographies.

Some basic ideas are tossed in the research pot below:

For USA major grocery, hardware, clothing etc. retailers what is security footage retention inside the locations, prefer list if available.

For USA major bank chains what is security footage retention inside the locations and at the ATM, prefer list if available.

Which USA major banks use facial recognition databases like in-house, Clear or ID.me, amazon one and are they shared? Do they keep photos of customer IDs?

It is rumored that Lowes & Macys & Apple iPhones and maybe others create secret facial recognition databases that are kept indefinitely, but that most refuse to directly reveal just what they are doing, prefer list if available.

Who are the main vendors that run facial recognition databases for retailers?

Which major retailers actually use these facial recognition databases from third party vendors and are they shared?

Where does the feed from USA traffic cameras go and what is it used for?

How police can reconstruct a person's entire driving route using traffic cameras or cell location data?

How long is license-plate info from traffic cameras data typically stored in the USA?

How do criminals sometimes try to evade traffic camera tracking?

Are traffic cameras in squad cars a continuous live feed into ALPR/ANPR systems regardless of whether the squad is in motion or the driver is out of the vehicle?

Are USA traffic camera feeds ever used for facial recognition?

What is the position of hidden cameras in modern cars?

What is the position of hidden microphones in modern cars?

What are modern cars recording surveillance systems?

Is there an industry standard AV format for the footage taken by secret cameras in modern cars?

Is retrieval of the footage taken by secret cameras in modern cars always done by the dealer and is it logged?

How do police or manufacturers sometimes extract hidden pre-crash video buffers, and which brands actually store the most camera footage?

The multiple hidden cameras and microphones secreted in modern cars are often unknown to the owner. Who gets to watch and listen to these recordings, how long are they retained, and does the car stop working if they are disabled?

What kind of legal protection in the USA exists for privacy, admissibility, or civil damages when harm is done with audio or video data that is secretly gathered and abused?

And stepping back for a broader view:

How believable are the providers of this new surveillance capitalism?

FIRST ChatGPT QUERY

ChatGPT query="For USA major grocery, hardware, clothing etc retailers what is security footage retention inside locations, prefer list if available." Below is a **practical overview of security-camera retention inside major U.S. retail chains** (grocery, big-box, hardware, clothing). Exact periods are rarely public and can vary by store size, region, and camera system, but asset-protection professionals and industry guidance provide approximate ranges.

Typical Security Footage Retention (U.S. Retail)

Most U.S. retail stores operate **rolling storage** systems (DVR/NVR) that overwrite old footage.

Store type	Typical retention
Small retail shops	7–30 days
Supermarkets / general retail	**30–90 days (most common)**
High-theft retail (electronics, jewelry)	90–180 days
Archived incident footage	1–5+ years

These ranges exist mainly due to storage costs and the need to investigate incidents within a reasonable timeframe.

Major U.S. Retailers (Approximate Known/Reported Ranges)

Retailer	Category	Typical retention inside store	Notes

Walmart	Grocery / big-box	~30 days to **6–12+ months** depending on store	Larger supercenters can keep footage up to a year or more; parking lots often 30–90 days.
Target			
Big-box / grocery			
~30 days			
Retention may vary by store and system.			
Costco	Warehouse club	~30 days typical	Some locations shorter for parking areas (reported by LP employees / incident cases).
Kroger / Albertsons-type grocery chains	Supermarket	~30–90 days	Typical grocery-industry retention window.
Home Depot	Hardware	~30–90 days	Similar to general retail CCTV retention (not publicly published).
Lowe's	Hardware	~30–90 days	Standard retail DVR/NVR rolling retention.
Best Buy	Electronics	~60–180 days possible	Higher-risk merchandise sometimes increases retention length.
Macy's / Nordstrom	Department store	~30–90 days	Standard retail range.
TJX (TJ Maxx / Marshalls)	Clothing discount	~30–90 days	Typical corporate retail surveillance policies.
Walgreens / CVS	Pharmacy retail	~30–90 days	Pharmacies sometimes retain register cameras longer for compliance.

Differences Inside the Same Store

Retention is **not uniform across cameras**.

Typical pattern:

Location in store	Retention
Checkout lanes / cash handling	longest retention
entrances/exits	medium
sales floor aisles	medium
parking lots	shortest

Reasons:

- evidence for fraud / chargebacks
- storage constraints
- resolution differences.

When Footage Is Kept Longer

Retailers **export or archive clips** if there is:

- shoplifting investigation
- employee theft investigation
- accident / injury claim
- police request or subpoena
- civil litigation

Those clips can be kept **years** for legal evidence.

Key Practical Points

- **30–90 days is the dominant baseline** across U.S. retail.

- Larger chains sometimes store **6–12 months locally or centrally**.
- Parking lot cameras usually have **shorter retention**.
- If footage is needed, requests usually must be made **within days or weeks** before overwrite.

✅ **Quick rule of thumb used by investigators**

Time after incident	Likelihood footage still exists
<7 days	very likely
7–30 days	usually available
30–90 days	depends on chain
>90 days	rare unless archived

If you want, I can also compile a **much deeper list (20–30 specific chains)** including grocery, hardware, apparel, and convenience retailers with the **best known retention estimates used by loss-prevention teams.** This can be useful if you're doing investigations or OSINT.

NEXT NEW ChatGPT QUERY

ChatGPT query= “For USA major bank chains what is security footage retention inside locations and at ATM, prefer list if available”
In the U.S., **there is no single federal rule specifying exactly how long banks must retain surveillance video**, but industry practices are fairly consistent. Most large bank chains follow similar internal security policies based on fraud investigation timelines and storage limits.

Below is a **typical retention overview for major U.S. bank chains (e.g., JPMorgan Chase, Bank of America, Wells Fargo, Citibank, U.S. Bank)**. These values are approximate because exact policies are rarely public.

Typical Security Footage Retention — Major U.S. Banks

Location / Camera Type	Typical Retention	Notes
ATM cameras (bank-owned ATMs)	**90 days minimum**	Industry baseline for fraud investigations.
	6–12 months common	Many large banks extend retention for ATM areas.
ATM vestibule cameras	**90–180 days typical**	Higher risk area; sometimes longer retention.
Inside branch – teller line cameras	**30–90 days typical**	Standard branch surveillance retention.
Lobby / general interior cameras	**30–90 days typical**	Often overwritten automatically.
Drive-through teller cameras	**90–180 days**	Usually retained longer due to transaction disputes.
Flagged incidents (fraud, robbery, subpoena)	**Years (case-dependent)**	Footage is archived once flagged.

ATM Retention (More Specific Industry Estimates)

Typical ranges mentioned across security and banking sources:

- **30–90 days:** most common default overwrite cycle.

90 days minimum: common institutional policy baseline.

6–12 months: many bank-owned ATM networks.

Up to 7 years: if footage is tied to investigation/legal case.

Differences by ATM Ownership

ATM Type	Typical Retention
Bank branch ATM	90 days – 1 year
Bank drive-up ATM	90–180 days
Retail ATM (gas station, bar)	30–90 days
Independent ATM operators	30–90 days

How Footage Is Actually Stored

Common operational details in large banks:

- Continuous recording but **auto-overwrite cycle** when storage fills.

Some systems **store high-resolution for ~90 days**, then keep **lower-resolution archival copies longer**.

Access restricted to **security/fraud teams** and logged for audit.

✅ **Practical takeaway:**

Area	Most realistic expectation
ATM transaction video	**90 days – 6 months**
Inside bank cameras	**30 – 90 days**
If incident reported	**retained indefinitely (case archive)**

If you want, I can also list **known ATM surveillance retention policies reported for specific banks (Chase, BofA, Wells Fargo, etc.) from court cases and security vendor documents**—those sometimes reveal **exact retention numbers** that banks normally don't publish.

NEXT NEW ChatGPT QUERY

ChatGPT query="Which USA major banks use facial recognition databases like in-house, Clear or ID.me, amazon one and are they shared? Do they

keep photos of customer IDs?”

Short answer: **Most major U.S. banks do NOT run large facial-recognition databases of customers the way companies like Clearview AI do.** But they **may collect photos of IDs and sometimes selfies for identity verification (KYC)**. These are typically used **one-to-one verification**, not large “searchable face databases.” The details vary depending on the bank and the identity-verification vendor they use.

Below is a breakdown of the main pieces.

---

1. Do major U.S. banks use facial recognition?

Yes — but mostly in **limited verification scenarios**, not mass identification.

Typical uses:

- **Mobile login authentication** (FaceID/Android biometrics)
- **Online account opening (selfie + ID match)**
- **Fraud detection / account recovery**

Examples:

- USAA pioneered mobile facial biometric login around 2015.

Wells Fargo and U.S. Bank allow customers to use their phone’s facial recognition for login.

Important:

- In most cases **the biometric template is stored on the phone**, not the bank’s servers.

So the bank **never receives the raw faceprint** in those cases.

---

2. Do banks keep photos of customer IDs?

Usually **yes, at least temporarily**, because of U.S. law.

Under **Customer Identification Program (CIP)** rules in the USA (part of KYC requirements):

- Banks must **verify identity**
- They must **keep records of how they verified it**.

That means banks commonly store:

- scanned driver's license/passport
- ID number
- sometimes the **ID photo**

Retention varies (often **5+ years after account closure** due to regulatory rules).

---

3. Vendors used by banks for selfie / ID verification

Many banks outsource identity verification to specialized vendors instead of building their own database.

Common vendors:

Document + selfie matching

- Mitek Systems
  - Used by many banks for mobile onboarding (selfie + ID match).

Facial verification / biometrics

- iProov (liveness detection)
- Clear Secure (biometric identity platform)
- ID.me (government + online identity network)

These systems typically do **1-to-1 matching**:

- selfie → compared to ID photo
- not matched against a large population database.

---

4. ID.me specifically

ID.me does something closer to a **central identity platform**.

Key facts:

- Uses facial recognition to match a **selfie to a government ID**.

Sometimes performs **one-to-many matching** to detect fraud accounts.

Keeps uploaded selfies for **about 7.5 years after account closure**.

But it's **mostly used by government agencies**, not widely by large retail banks.

---

5. CLEAR in financial services

Clear Secure is expanding into banking and financial identity.

Their model:

- user uploads **government ID + selfie**
- identity becomes reusable across partners.

However:

- adoption by **major U.S. banks is still limited** (more common in fintech, real estate, and payments so far).

---

6. Amazon One

Amazon One is a **palm-recognition payment system**, not facial recognition.

Use today:

- retail stores
- stadiums
- some payment terminals

There's **no evidence major U.S. banks use Amazon One for customer identity verification**.

---

7. Do banks share biometric databases?

Generally **no shared facial database across banks**.

Typical structure:

Data type	Shared?	Notes
ID documents	sometimes	via verification vendors
Fraud signals	yes	via fraud networks
Face biometrics	usually no	kept vendor-side or device-side

Banks do share **fraud and account-risk data** through systems like:

- Early Warning Services (owned by large banks) which helps detect fraud and operates Zelle.

But this **does not include a national facial recognition database**.

---

8. Key takeaway

Typical U.S. bank identity process:

1. Upload ID (driver's license/passport)
2. Take selfie
3. Vendor checks:
    - ID authenticity

- selfie matches ID
- liveness test

4. Bank stores **verification record + ID image**
5. Face template may be deleted or kept by vendor

This is **not the same as police or surveillance facial recognition systems**.

✅ Summary

Question	Reality
Do banks use facial recognition?	Sometimes, mostly for ID verification
Do they store customer photos?	Often yes (ID scans)
Do they maintain face databases?	Usually no
Do they share biometric data across banks?	Rare
Are Clear / ID.me widely used by big banks?	Limited adoption

✔ If you want, I can also list **which specific U.S. banks use selfie verification vendors (Mitek, Socure, Jumio, etc.)** — that list is actually more revealing than the big bank names themselves.

You're now using our basic model.
To access more intelligence, create an account or log in.

Sources

- AB

  American Banker

  Pressure grows on banks to abandon facial recognition tech | American Banker

  May 2, 2021

  W

Wikipedia

Know your customer

Mitek Systems

ID.me

CS

CyberScoop

ID.me CEO backtracks on claims company doesn't use powerful facial recognition tech | CyberScoop

January 25, 2022

identity.clearme.com

CLEAR & Alloy Partnership Announcement | CLEAR

October 17, 2024

Investopedia

Early Warning Services: Identity, Payment Solutions, & Zelle Ownership

January 25, 2023 — Early Warning Services LLC is a financial technology (fintech) firm owned by seven major U.S. banks: Bank of America, Capital One, JPMorgan Chase, PNC Bank, Truist, U.S. Bank, and Wells Fargo. It specializes in identity verification, fraud prevention, and payment solutions, and it operates the widely used Zelle money transfer app. Originally established as a consumer reporting agency, the company helps banks and financial institutions manage risk by sharing consumer banking and transaction data. Early Warning provides services to over 2,500 financial institutions, government entities, and payment companies. While it does not generate credit scores, it compiles consumer banking history data that help institutions decide on offering banking products. Consumers can request a free report once a year under the Fair Credit Reporting Act. Zelle, launched in 2017 as a competitor to systems like Venmo and PayPal, enables instant, fee-free money transfers and processed over $155

billion in Q2 of 2022 alone. Early Warning has evolved through the decades, expanding from check verification to broader digital and fraud detection services, solidifying its key role in secure, real-time financial transactions.

More

- ⚖️

legalclarity.org

How Does KYC Work: Identity Verification and Compliance - LegalClarity

February 28, 2026 — HOW DOES KYC WORK: IDENTITY VERIFICATION AND COMPLIANCE Learn how financial institutions verify your identity through KYC, what documents you'll need, and what happens if your application gets flagg...

newmoneyreview.com

US banks are exposed to a fake ID crimewave - New Money Review

January 20, 2026 — US BANKS ARE EXPOSED TO A FAKE ID CRIMEWAVE Written by Timur Yunusov on January 21, 2026 Criminals are weaponising artificial intelligence (AI) to create millions of fake bank accounts, used in mon...

arsa.technology

Data Protection in Banking: Leveraging Face Recognition API for KYC Compliance

January 9, 2026 — DATA PROTECTION IN BANKING: LEVERAGING FACE RECOGNITION API FOR KYC COMPLIANCE Navigate banking compliance with ARSA's Face Recognition API. Learn how to secure KYC verification, protect data, and p...

factually.co

Fact Check: How do USA banks plan to implement biometric authentic...

November 7, 2025 — HOW DO USA BANKS PLAN TO IMPLEMENT BIOMETRIC AUTHENTICATION FOR ACCOUNT ACCESS? Checked on November 8, 2025 Disclaimer: Factually can make mistakes. Please verify important info or breaking news. L...

idtechwire.com

FNF Integrates CLEAR Biometric Verification to Secure Real Estate Closings - ID Tech

September 8, 2025 — FNF INTEGRATES CLEAR BIOMETRIC VERIFICATION TO SECURE REAL ESTATE CLOSINGS September 9, 2025 Fidelity National Financial (FNF), the largest title insurance provider in the United States, has partne...

ainvest.com

FNF partners with CLEAR to combat real estate fraud with biometric identity verification.

September 8, 2025 — FNF PARTNERS WITH CLEAR TO COMBAT REAL ESTATE FRAUD WITH BIOMETRIC IDENTITY VERIFICATION. ByAinvest Tuesday, Sep 9, 2025 7:39 am ET 1min read • FNF partners with CLEAR Secure for biometric identit...

AIJ

aijourn.com

Fidelity National Financial Announces Partnership with CLEAR to Fight Real Estate Fraud | The AI Journal

September 8, 2025 — FIDELITY NATIONAL FINANCIAL ANNOUNCES PARTNERSHIP WITH CLEAR TO FIGHT REAL ESTATE FRAUD Cision PR Newswire 9 September 2025 4 minutes read iframe FNF Has Launched the First Phase of Biometric Ide...

biometricupdate.com

US Corporate Transparency Act rollbacks create customer ID verification needs | Biometric Update

April 15, 2025 — US CORPORATE TRANSPARENCY ACT ROLLBACKS CREATE CUSTOMER ID VERIFICATION NEEDS Apr 16, 2025, 5:59 pm EDT | Jack Shaw Categories Biometrics News | Financial Services Image: US Corporate Transparen...

idtechwire.com

CLEAR Partners with Stripe to Transform Digital Identity Payment Systems - ID Tech

March 24, 2025 — CLEAR PARTNERS WITH STRIPE TO TRANSFORM DIGITAL IDENTITY PAYMENT SYSTEMS March 25, 2025 Stripe, the global financial technology platform, has announced a comprehensive partnership with CLEAR to man...

biometricupdate.com

ConnectID, Visa, ID.me illustrate central place digital ID plays in digital economy | Biometric Update

January 27, 2025 — CONNECTID, VISA, ID.ME ILLUSTRATE CENTRAL PLACE DIGITAL ID PLAYS IN DIGITAL ECONOMY Digital identity can address identification gap for rural, low-income populations Jan 28, 2025, 4:08 pm EST | Joe...

cyberlink.com

How Facial Recognition Identity Verification Enhances Smart Banking

November 7, 2024 — HOW FACIAL RECOGNITION IDENTITY VERIFICATION ENHANCES SMART BANKING Fintech Nov 08, 2024 Mobile banking has alleviated the inconvenience of having to physically visit a bank during opening hours....

linkedin.com

Use of AI in KYC in Banking

August 18, 2024 — 5. Deutsche Bank * Application Areas: Customer due diligence, risk scoring, transaction monitoring, ongoing compliance, blacklist screening, address, phone, and picture verification. * Technical Solu...

comperemedia.com

Lightbulb Moments: Spark Your Strategy (Vol. 15)

July 28, 2024 — 1. # Lightbulb Moments: Spark Your Strategy (Vol.15) Published: July 29, 2024 Copied to clipboard 9 minutes read Comperemedia's Chief Insights Officer, Andrew Davidson is well known for sharing t...

nttdata.com

Amazonification of banks: Embracing data, personalization and innovation | NTT DATA

June 19, 2024 — AMAZONIFICATION OF BANKS: EMBRACING DATA, PERSONALIZATION AND INNOVATION * June 20, 2024 Image: abstract digital ribbon In today's digital era, the influence of tech giants like Amazon extends bey...

investing.com

CLEAR partners with Public for speedy ID checks By Investing.com

May 29, 2024 — CLEAR PARTNERS WITH PUBLIC FOR SPEEDY ID CHECKS EditorNatashya Angelica Published 05/30/2024, 12:14 PM View all comments (0) Image: CLEAR partners with Public for speedy ID checks NEW YORK - CLE...

AB

AB

americanbanker.com

JPMorgan details its invisible role with Amazon — and others | American Banker

May 1, 2024 — JPMORGAN DETAILS ITS INVISIBLE ROLE WITH AMAZON — AND OTHERS By Kate Fitzgerald CloseText | About Kate twitter | plasticpayments mailto | kate.fitzgerald@arizent.com linkedin | https://www.li...

cyberlink.com

KYC Becomes eKYC with the Addition of Facial Recognition in the BFSI Industry | FaceMe | CyberLink

April 17, 2024 — HOW DO BIOMETRIC IDENTIFICATION TECHNOLOGIES COMPARE? Financial institutions are increasingly using advanced technologies to ensure the security of their assets. The three main technologies used in e...

idtechwire.com

With Sora ID Acquisition, CLEAR Comes to Financial Services - ID Tech

October 5, 2023 — WITH SORA ID ACQUISITION, CLEAR COMES TO FINANCIAL SERVICES October 6, 2023 CLEAR, known for its biometric airport screening and venue access program, has marked its entry into the financial servic...

bank.ax

CLEAR launches reusable KYC solution - Bank.ax - Fintech, Banking, Innovations

October 4, 2023 — Image: CLEAR launches reusable KYC solution CLEAR LAUNCHES REUSABLE KYC SOLUTION CLEAR LAUNCHES REUSABLE KYC SOLUTION Image: CLEAR Logo WHAT IS KYC? Know Your Customer (KYC) is a process used b...

financialit.net

CLEAR Expands Into Financial Services, Launches Its First Reusable KYC Solution with Fast, Frictionless Consumer Experience | Financial IT

October 4, 2023 — CLEAR EXPANDS INTO FINANCIAL SERVICES, LAUNCHES ITS FIRST REUSABLE KYC SOLUTION WITH FAST, FRICTIONLESS CONSUMER EXPERIENCE * Digital Identity * 05.10.2023 08:25 am Today, CLEAR, the secure identit...

amazon.com

How Amazon Finance Technologies simplified global payments by creating a payments repository using Amazon DocumentDB | AWS Database Blog

December 13, 2022 — HOW AMAZON FINANCE TECHNOLOGIES SIMPLIFIED GLOBAL PAYMENTS BY CREATING A PAYMENTS REPOSITORY USING AMAZON DOCUMENTDB by Pradeep Misra and Balaji Kumar Gopalakrishnan on 14 DEC 2022 in Amazon Documen...

americanbanker.com

How Amazon, Apple, Facebook, Google are infiltrating financial services | American Banker

March 28, 2022 — HOW AMAZON, APPLE, FACEBOOK, GOOGLE ARE INFILTRATING FINANCIAL SERVICES ByMiriam Cross March 29, 2022 9:00 PM * Facebook * Twitter * LinkedIn * Email Image: Logos for Amazon, Apple and Google Me...

nextgov.com

Agencies shouldn't use facial recognition for ID verification, groups say - Nextgov/FCW

February 14, 2022 — AGENCIES SHOULDN'T USE FACIAL RECOGNITION FOR ID VERIFICATION, GROUPS SAY ImageImage Getty Images By Natalie Alms, Senior Correspondent, Nextgov/FCW, FCW By Natalie Alms, FCW | February 15, 2022...

id.me

ID.me Announces Options for Selfie Deletion and Identity Verification without Automated Facial Recognition - ID.me Network

February 7, 2022 — ID.ME ANNOUNCES OPTIONS FOR SELFIE DELETION AND IDENTITY VERIFICATION WITHOUT AUTOMATED FACIAL RECOGNITION February 8, 2022 By: ID.me COMPANY COMMITTED TO DELIVERING GOVERNMENT SOLUTIONS THAT MAXI...

wired.com

The IRS Drops Facial Recognition Verification After Uproar | WIRED

February 7, 2022 — Jon Brodkin, Ars Technica Business Feb 8, 2022 4:26 PM THE IRS DROPS FACIAL RECOGNITION VERIFICATION AFTER UPROAR Privacy advocates and lawmakers from both major parties objected to the agency's...

yahoo.com

The IRS will move away using ID.me's facial recognition verification for IRS.gov

February 6, 2022 — THE IRS WILL MOVE AWAY USING ID.ME'S FACIAL RECOGNITION VERIFICATION FOR IRS.GOV Caroline Haskins Updated Mon, February 7, 2022 at 8:20 PM UTC 3 min read Image * The IRS will eventually stop usi...

aclu.org

Three Key Problems with the Government's Use of a Flawed Facial Recognition Service | American Civil Liberties Union

February 1, 2022 — THREE KEY PROBLEMS WITH THE GOVERNMENT'S USE OF A FLAWED FACIAL RECOGNITION SERVICE Forcing people to use private ID-verification to access tax accounts or other government services raises serious p...

AB

AB

americanbanker.com

Facial recognition tech is catching on with banks | American Banker

September 12, 2021 — FACIAL RECOGNITION TECH IS CATCHING ON WITH BANKS By David Heun CloseText | About David twitter | PaymentsDave mailto | david.heun@arizent.com linkedin | daveheun September 13, 2021, 2:30 p....

AB

AB

americanbanker.com

Will banks get caught up in facial recognition backlash? | American Banker

February 17, 2020 — WILL BANKS GET CAUGHT UP IN FACIAL RECOGNITION BACKLASH? By Penny Crosman CloseText | About Penny twitter | pennycrosman mailto | penny.crosman@arizent.com linkedin | pennycrosman February 1...

axios.com

Biometrics are being used more in banking and retail, raising privacy concerns

February 17, 2020 — Feb 18, 2020 - Economy BIOMETRICS INVADE BANKING AND RETAIL Image * Jennifer A. Kingson Image: Illustration of a fingerprint with a dollar sign. Illustration: Eniola Odetunde/Axios Banks have...

biia.com

Amazon eyes underbanked customers with checking account partnership talks | BIIA.com

March 23, 2018 — AMAZON EYES UNDERBANKED CUSTOMERS WITH CHECKING ACCOUNT PARTNERSHIP TALKS Mar 24, 2018 | ! Homepage Slider, Amazon, Inclusion, Online Lending, SME Access to Finance Issue, United States | | Online...

AB

americanbanker.com

Is Amazon’s Alexa ready for P2P payments? | American Banker

March 18, 2018 — But Amazon, Google and Apple don’t yet have that capability in their smart speakers. Neither company will store the voiceprints necessary to do voice recognition, said Al Pascual, senior vice preside...

CNBC

cnbc.com

Amazon's talks with JP Morgan may build on services to the unbanked

March 4, 2018 — AMAZON WANTS TO MAKE IT EASIER TO SHOP ITS WEBSITE WITHOUT A CREDIT CARD Published Mon, Mar 5 2018 3:34 PM EST Updated Mon, Mar 5 2018 4:01 PM EST Image: thumbnail Lauren Hirsch@laurenshirsch Ke...

bayometric.com

Biometric Authentication for Customer Verification (KYC)

May 25, 2017 — BENEFITS OF USING BIOMETRICS FOR KYC MANAGEMENT IN THE BANKING INDUSTRY Biometric technology is very well suited to the banking industry and offers significant advantages for the bank and end user al...

aws

amazon.com

Fully Managed AI Service – Amazon Rekognition Identity Verification – AWS

IDENTITY VERIFICATION USING AMAZON REKOGNITION Verify user identity online using ML Deploy a solution template Contact us Amazon Rekognition * Overview * Pricing WHY IDENTITY VERIFICATION? In-...

amazon.com

Amazon One

cleared.id

Partner with Us | Cleared®

PARTNER WITH CLEARED® Help us build a trusted, verified digital economy for Jamaica and the wider Caribbean. Cleared® works with organisations, platforms, regulators and customers who believe that i...

nfcw.com

Know Your Customer (KYC) news • NFCW

GOOGLE DETAILS ITS PLAN TO OFFER FREE US BANK ACCOUNTS VIA GOOGLE PAY By Sarah Clark • 19 November 2019 • Updated 19 November 2019 US consumers will be able to start signing up for checking accounts...

clearidsteps.org

clearidsteps.org/traditional-banking

* * * * * Traditional banking IDENTITY SECURED. FRAUD UNMASKED. COMPLIANCE ACHIEVED. Meet local and global regulatory requirements and fight fraud without compromising on security or custom...

cleardil.com

ClearDil Identity Verification – Secure & Compliant

WHAT IS IDENTITY VERIFICATION? Identity verification, also known as ID verification, is the process of confirming that a customer is who they claim to be. It uses official government-issued identity...

amazon.eu

Verifying your identity

Register to get the Amazon Pay button on your site or app. Note Buyers don't need to register. During checkout, they use their existing Amazon account credentials. VERIFYING YOUR IDENTITY Your Ama...

americanexpress.com

Terms and Conditions | Amazon One | American Express

TERMS AND CONDITIONS FOR USING AMERICAN EXPRESS CARDS IN AMAZON ONE Last Modified: March 2023 Amazon One is a service offered by Amazon.com Services, Inc. ("Amazon") whereby individuals can id...

bain.com

Banking's Amazon Moment | Bain & Company

Brief BANKING'S AMAZON MOMENT BANKING'S AMAZON MOMENT Alexa, move my bank account to Amazon. By Gerard du Toit and Aaron Cheris * min read * * * } Brief BANKING'S AMAZON MOMENT * * *...

NEXT NEW ChatGPT QUERY

ChatGPT query="It is rumored that Lowes & Macys & Apple iphones and maybe others create secret facial recognition databases that are kept indefinitely, but that most refuse to directly reveal just what they are doing, prefer list if available."

There **is some truth mixed with rumor** in the claim that companies like Lowe's, Macy's, or Apple create secret facial-recognition databases. The reality is:

- Some retailers **have used facial recognition systems**.
- Many **refuse to clearly disclose details** (or say the information is "proprietary").
- In most cases the systems are intended for **security or loss-prevention**, not general customer tracking—but critics worry databases could persist or expand.

Below is a **fact-based list of companies reported to use, test, or be accused of using facial recognition in stores**, based on investigations and advocacy reports.

Retailers reported to use facial recognition (or have used it)

Confirmed or acknowledged at some point

Lowe's – said it used facial recognition to identify known shoplifters in stores.

Macy's – listed in multiple reports as deploying facial recognition systems in stores.

Apple – reported in advocacy scorecards as using facial recognition in some retail locations.

Albertsons – identified as using facial recognition technology in stores.

Ace Hardware – included in reports of retailers deploying the technology.

H-E-B Grocery – also reported using in-store facial recognition.

Rite Aid – ran facial recognition systems in hundreds of stores for years to identify suspected shoplifters.

Recent news example:

Wegmans – stores in New York warn customers that facial scans and other biometric identifiers may be stored for security purposes.

Retailers that refused to answer whether they use it

Investigations have found many companies simply **declined to disclose** whether they scan customers' faces:

- Walmart
- Best Buy
- Publix
- Walgreens Boots Alliance
- TJX Companies (T.J. Maxx / Marshalls)
- McDonald's

Many told investigators the information was **"proprietary" or declined to comment**, leaving their practices unclear. Why would that be? Could it be an NDA?

Companies that have said they do NOT use it

Some retailers publicly stated they **do not deploy facial recognition** in stores:

- Ahold Delhaize (Food Lion, Stop & Shop, etc.)
- Target (later confirmed not using it in some reports)
- Costco
- Home Depot
- CVS
- Dollar Tree
- Verizon

(Some companies change policies over time.)

Important nuance about “secret databases”

Most documented retail systems:

- **Compare faces against a small database** of suspected shoplifters or banned individuals.
- Often **delete non-matching faces** quickly (according to company statements).
- Are typically run by third-party vendors such as security analytics firms.

However critics warn that:

- Data retention policies are often **unclear or undisclosed**.
- Databases can potentially be **shared across stores or with law enforcement**.

✅ **Bottom line:**

- Facial recognition in retail **does exist and has been deployed by several chains**.
- Many companies **won’t disclose details**, which fuels rumors about large secret databases.
- Evidence usually points to **loss-prevention watchlists**, not massive permanent databases of every shopper—but transparency is limited.

✔ If you want, I can also show:

- A **much longer list of companies experimenting with facial recognition globally (stores, airports, stadiums, casinos)**

- Or the **main vendors that run these databases for retailers** (often more important than the stores themselves).
-

American Civil Liberties Union

Are Stores You Shop at Secretly Using Face Recognition on You? | American Civil Liberties Union

March 25, 2018

Common Dreams

Rights Coalition Demands US Retailers Reject Use of Facial Recognition | Common Dreams

July 13, 2021

CNBC

Rite Aid deployed facial recognition in hundreds of U.S. stores

July 27, 2020

New York Post

NYC Wegmans' storing shoppers' facial scans and biometric data to ID customers, boost security: 'We understand concerns'

January 5, 2026 — Wegmans grocery stores in Brooklyn and Manhattan have begun collecting and storing biometric data, primarily facial recognition scans, to enhance security and identify

individuals previously flagged for misconduct. The initiative, launched after a 2024 pilot program that initially promised not to store data, now includes notices alerting customers that their biometric information may be retained, though Wegmans asserts it does not sell or trade this data. While the chain stresses that the technology is only used in select high-risk stores, privacy advocates and lawmakers have raised concerns about potential bias and misuse, citing past incidents, including Rite Aid's wrongful facial recognition identifications and Madison Square Garden's banning of critics. Although a 2021 New York City law mandates signage for biometric data use, it lacks enforcement power. A City Council bill to ban biometric collection failed, but advocacy continues amid growing concerns over privacy, fairness, and data retention practices. Wegmans claims to use the data strictly for security purposes, with safeguards in place to mitigate bias.

Fight for the Future

New Report and Scorecard Shows Which Retailers Are Using Facial Recognition on Shoppers, Employees

May 24, 2021

American Civil Liberties Union

Retailers Secretively Using Face Recognition to Spot "Persons of Interest" — Including For the Government | American Civil Liberties Union

January 19, 2026

More

gothamist.com

Not just Wegmans: More NYC retailers using facial recognition as tech outpaces law - Gothamist

January 11, 2026 — News NOT JUST WEGMANS: MORE NYC RETAILERS USING FACIAL RECOGNITION AS TECH OUTPACES LAW Image: Signs advertise the use of facial recognition technology at Macy's in Herald Square. Paige Oamek /...

rnz.co.nz

Facial recognition technology supported by big name retailers | RNZ News

June 14, 2025 — 15 Jun 2025 FACIAL RECOGNITION TECHNOLOGY SUPPORTED BY BIG NAME RETAILERS 6:05 pm on 15 June 2025 Image: Phil Pennington Phil Pennington, Reporter Image: Stylised illustration of biometric data...

ny1.com

Kroger denies reports of in-store facial recognition devices

January 27, 2025 — A Kroger spokesperson said the store is not using facial recognition technology in connection with electronic shelf labels or pricing. (Spectrum News 1/Geraldine Torrellas) KROGER DENIES REPORTS OF...

fightforthefuture.org

Civil Rights Groups Call on Stores to Reject Facial Recognition

July 13, 2021 — CIVIL RIGHTS GROUPS CALL ON STORES TO REJECT FACIAL RECOGNITION FOR IMMEDIATE RELEASE: Wednesday, July 14, 5:30 am ET Contact: Caitlin Seeley George, caitlin@fightforthefuture.org As Albertsons, Lo...

theregister.com

Facial-recognition technology gets a smack in the chops from civil rights campaigners • The Register

July 13, 2021 — This article is more than 1 year old FACIAL-RECOGNITION TECHNOLOGY GETS A SMACK IN THE CHOPS FROM CIVIL RIGHTS CAMPAIGNERS US RETAILERS ACCUSED OF PRIVACY INVASION Image Updated Civil rights camp...

kioskmarketplace.com

Civil rights groups call on retailers to halt facial recognition | Kiosk Marketplace

July 13, 2021 — CIVIL RIGHTS GROUPS CALL ON RETAILERS TO HALT FACIAL RECOGNITION Image Image provided by iStock. July 14, 2021 More than 35 civil rights organizations are calling for retailers to not use facial...

sado.org

SADO - Article - Apple iPhone Surveillance & Facial Recognition in Retail Stores

APPLE IPHONE SURVEILLANCE & FACIAL RECOGNITION IN RETAIL STORES Apple iPhone Surveillance Recent news that Apple plans to scan Apple devices for images of Child Sexually Abusive Material (CSAM) h...

NEXT NEW ChatGPT QUERY

ChatGPT query="Who are the main vendors that run facial recognition databases for retailers"

Retailers that use **facial recognition watchlists or shared "offender databases"** typically don't build the systems themselves. They rely on specialized **retail-security / biometrics vendors** that supply software to scan faces from CCTV cameras and compare them against a **database of "persons of interest" (often suspected shoplifters or banned individuals)**.

Below are some of the **main vendors and platforms currently used by retailers**.

Major vendors running facial-recognition systems for retailers

1. Facewatch

- UK-based system widely used by retail chains and convenience stores.
- Maintains a **shared database of individuals flagged by participating retailers**.
- When someone enters a store, cameras scan their face and match it to the database; staff receive an alert if there's a hit.
- Some deployments reportedly contain **100,000+ individuals across retailers**.

Use cases

- Convenience stores and supermarkets (especially in the UK)
- Retail crime prevention networks across multiple businesses

---

2. FaceFirst

- One of the most well-known **U.S. retail facial recognition platforms**.
- Integrates with existing CCTV and creates **watchlists of repeat offenders or persons of interest**.
- Sends real-time alerts when someone on the list enters a store.

Clients / contexts

- Large retail chains
- Shopping malls and casinos
- Retail loss-prevention teams

---

3. Auror

- A **retail crime intelligence platform** used by major chains in the U.S., UK, Australia, and New Zealand.
- Not purely facial recognition, but integrates **incident reporting, suspect images, and shared intelligence between retailers and police**.
- Often combined with other biometric systems to build a **networked offender database**.

---

4. FaiceTech

- UK startup deploying **live facial recognition for supermarkets and retail environments**.
- Matches shopper images against a **watchlist compiled by the retailer**.
- Example: pilot deployments in supermarkets scanning customers at entry points.

---

5. Corsight AI

- Israeli computer-vision company providing **real-time facial recognition for security and retail environments**.
- Designed to work with existing cameras and identify individuals even in difficult conditions (low light, partial faces).

---

6. NEC (NeoFace platform)

- Japanese multinational offering **NeoFace Watch for Retail**, a biometric recognition system integrated with store CCTV.
- Used globally for security and sometimes customer-identification programs.

---

7. Gatekeeper Systems + ROC AI

- Loss-prevention platform integrating **facial recognition algorithms with retail security systems**.
- Generates alerts when someone on a retailer's watchlist enters the store.

Other companies whose tech sometimes powers these systems

Some retailers license algorithms or infrastructure from broader biometric vendors:

IDEMIA – large biometric identity vendor supplying face recognition to governments and private companies.

Flock Safety – primarily license-plate recognition but also provides watchlist systems used by private businesses including retailers.

How these retail databases usually work

Typical architecture:

1. **Cameras at entrances** capture faces.
2. Software converts the image into a **biometric template**.
3. Template is matched against a **watchlist database** (shoplifters, banned customers, violent offenders).
4. If matched:
    - Staff receive an alert on phones or dashboards.
    - They may monitor or deny service.

Databases may be:

- **Single-retailer** (internal watchlist)
- **Shared network** across multiple retailers
- **Connected to police or retail crime platforms**

✅ **Important nuance:**

- Most vendors claim they **don't maintain a universal global database**; instead they host **separate watchlists created by each retailer or network of retailers**.
- However, systems like Facewatch or Auror enable **cross-retailer intelligence sharing**, which can effectively function like a shared database.

✔ If you want, I can also explain:

- **Which major retailers actually use these systems** (Walmart, UK convenience chains, malls, etc.).
- **How large these facial-recognition watchlists typically get** and whether they are shared between companies.

Sources

-

MISP Galaxy

Surveillance Vendor - MISP galaxy

Financial Times

UK high streets turn to facial recognition in fight against shoplifting

Today — In the UK, retailers are increasingly adopting facial recognition technology to combat the surge in shoplifting and violence against retail staff, which cost £2.2 billion in 2024. Following criticism of police inaction, companies have invested nearly £1 billion in security measures, including AI surveillance systems that identify repeat offenders in real time or retrospectively. Companies like Auror and Facewatch are leading providers, with Facewatch actively sharing a database of over 100,000 individuals across retailers. However, the approach has sparked privacy concerns and criticism over accuracy and potential misuse, especially after cases like that of Lavinia McIntyre, a former police officer mistakenly flagged and publicly accused. While some stores report declines in incidents, privacy advocates argue the technology lacks regulation and transparency, fearing a drift toward private-sector driven surveillance. The UK government is considering stricter retail crime laws and better regulation of biometric surveillance. Meanwhile, concerns grow about how retail workers are tasked with responding to alerts generated by opaque algorithms, raising both ethical and safety questions.

FaceFirst

Face matching software for retail stores

Biometric Update

Supermarket chain Asda chooses FaiceTech for facial recognition surveillance | Biometric Update

March 30, 2025

Corsight

Retail - Corsight

NEC New Zealand

NeoFace Watch for Retail - NEC New Zealand

Biometric Update

ROC facial recognition integrated by US retail loss prevention platform | Biometric Update

February 8, 2026

Wikipedia

IDEMIA

Flock Safety

More

-

kognition.ai

AI Security for Retail | Loss Prevention & Store Security | Kognition AI - Kognition AI

February 19, 2026 — 🛡️ KOGNITION APPLICATIONS FOR RETAIL 👥 PEOPLE DETECTION & COUNTING Kognition’s People application is the most versatile tool in the retail security arsenal, providing both loss prevention intelligen...

arsa.technology

API Showdown: Why ARSA's Face Recognition API is the Superior Choice for Retail Loss Prevention | ARSA Technology

September 2, 2025 — API SHOWDOWN: WHY ARSA’S FACE RECOGNITION API IS THE SUPERIOR CHOICE FOR RETAIL LOSS PREVENTION Image: api-showdown-why-arsas-face-recognition-api-is-the-superior-choice-for-retail-loss-prevention-w...

biometricupdate.com

Facewatch comes under the public eye again | Biometric Update

June 24, 2025 — FACEWATCH COMES UNDER THE PUBLIC EYE AGAIN Jun 25, 2025, 11:58 am EDT | Masha Borak Categories Biometrics News | Commercial Applications | Facial Recognition Image: Facewatch comes under the p...

nocamels.com

Israeli Facial Recognition Tech Deployed To Fight Shoplifting in US

September 26, 2024 — (Photo: Depositphotos) Israeli facial recognition developer Corsight AI has teamed up with American anti-shoplifting company RaptorVision in a global strategic partnership that will see the former’s...

biometricupdate.com

Facewatch, Vista CCTV deliver GDPR-compliant biometric surveillance solution for retail, hospitality | Biometric Update

February 11, 2020 — FACEWATCH, VISTA CCTV DELIVER GDPR-COMPLIANT BIOMETRIC SURVEILLANCE SOLUTION FOR RETAIL, HOSPITALITY Feb 12, 2020, 2:39 pm EST | Luana Pascu Image: Facewatch, Vista CCTV deliver GDPR-compliant biom...

racked.com

Facial Recognition Technology Is on the Rise in Retail - Racked

May 21, 2018 — YOUR FAVORITE STORES COULD BE TRACKING YOU WITH FACIAL RECOGNITION Stores are using technology that can match your face against a database of 25 million people in seconds. By Chavie Lieber May 22,...

securityvision.io

FaceFirst used in thousands of retail stores - Security Vision

January 1, 2018 — FACEFIRST USED IN THOUSANDS OF RETAIL STORES From Security Vision Summary --- 0 Products and Institutions: Product Deployed | FaceFirst (Software) Institutions ** | FaceFirst Datasets | FaceFir...

consumerreports.org

Facial Recognition: Who's Tracking You in Public? - Consumer Reports

FACIAL RECOGNITION: WHO'S TRACKING YOU IN PUBLIC? New technology is moving into the world of department stores, casinos, and cruise ships—and even churches. How freaked out should you be? Image: Co...

ottica.ai

Ottica AI | Retail

RETAIL LOSS PREVENTION IN RETAIL: PROTECT YOUR BOTTOM LINE WITH ADVANCED FACIAL RECOGNITION In today’s competitive retail landscape,

preventing losses is critical to maintaining profitability. Otti...

nec.co.nz

NeoFace Watch for Retail - NEC

HOW NEOFACE WATCH WORKS IN RETAIL Real-Time Monitoring NEC's NeoFace Watch leverages advanced facial recognition technology to continuously monitor entry points and in-store areas, accurately identi...

vixvizion.com

Retail Safety and Loss Prevention | Vix Vizion.com

* * * # Retail Safety and Loss Prevention Explore Vix Vizion's Retail Solutions using our world leading Imagus Facial Recognition Software to reduce Retail Crime and keep staff safe. Image PRI...

visionqueue.com

Vision Queue | Retail

1. Home INCREASE REVENUE BY PROVIDING EXCEPTIONAL CUSTOMER SERVICE The retail industry is a vast industry ranging from corner coffee shops to giant department stores. One of the main goals is to en...

oosto.com

Video Analytics & Facial Recognition Surveillance in Retail | Oosto

RETAIL REDUCE SHRINKAGE WITH REAL-TIME SHOPLIFTER IDENTIFICATION. Retailers are constantly preoccupied with trying to think of different, creative ways of increasing profits. Yet, oftentimes they d...

corsight.ai

Retail LP - Corsight

MAXIMIZE STORE SECURITY WITH YOUR EXISTING CAMERAS * Identify Individuals on Watchlists and Authorized Lists * Recognize Patterns of Shoplifting * Combat Sweethearting * Understand Customer Demograp...

enface.ai

Enface - Solutions: Retail

* * * * * * Request Demo Recognize VIPs and thieves, collect analytics on visitors and passers-by, and optimize personnel management - all to increase your sales and reduce costs. Face re...

dataintelo.com

Face-in-Crowd Search Market Research Report 2033

REGIONAL OUTLOOK From a regional perspective, North America continues to lead the Face-in-Crowd Search market, accounting for a market size of USD 0.91 billion in 2024. This dominance is underpinned...

NEXT NEW ChatGPT QUERY

ChatGPT query= "Which major retailers actually use these facial recognition databases from third party vendors and are they shared"

Yes—**some major retailers do use facial-recognition systems from third-party vendors**, but the situation is messy:

- many retailers **deny it**,
- some **tested it then stopped**,
- and others **actively use shared watchlist systems** for loss prevention.

Below is a breakdown of what's publicly known.

---

1. Major retailers confirmed or reported to use facial recognition

These examples come from investigations, company disclosures, or news reports.

Grocery / supermarket chains

Wegmans – uses facial recognition in some stores to identify "persons of interest" tied to theft or security incidents.

Albertsons – listed by advocacy groups as using facial recognition for security and fraud prevention.

Sainsbury's – trialing facial recognition in UK stores to identify shoplifters.

Department / big retail

Macy's – reported to use facial recognition in stores for security purposes.

Kohl's – appears in leaked lists of companies testing facial recognition tools such as Clearview AI.

Pharmacy / convenience

- **Rite Aid** – deployed facial recognition in **200 U.S. stores** over several years to identify suspected shoplifters.

Electronics / tech retail

- **Apple** – stores have used facial recognition systems for fraud or theft investigations.

Hardware

- **Lowe's** – confirmed to use facial recognition for identifying shoplifters.

---

2. Retailers that reportedly do NOT use it

Some big chains have publicly stated they **don't use facial recognition** in stores.

Examples include:

- **Walmart**
- **Target**
- **Kroger**
- **Home Depot**

These companies have said they **don't deploy facial recognition for surveillance**, though they still use regular cameras and analytics.

(Policies can change, and some retailers have tested it in pilots.)

---

3. Third-party vendors that supply the systems

Retailers often don't build these systems themselves—they buy them from vendors.

Common vendors include:

Facewatch – used by several UK retailers; identifies known offenders and sends alerts to staff.

Auror – retail crime intelligence platform where stores share incident data.

Clearview AI – facial-search tool used in trials by various companies and security teams.

These systems typically integrate with store CCTV.

---

4. Are the databases shared between retailers?

Sometimes yes—but **how depends on the vendor**.

Shared watchlists (multi-store networks)

Platforms like **Facewatch** or **Auror** allow retailers to share data about suspected offenders.

Typical model:

- store uploads image of a suspected shoplifter
- system creates a **watchlist entry**
- other stores using the platform receive alerts if that person appears

In some deployments the system can **link incidents across multiple retailers** in the network.

Internal-only databases

Other retailers keep databases **private to their own chain** (e.g., internal loss-prevention watchlists).

Law-enforcement integration

Sometimes:

- police provide photos
- retailers share evidence with police
- or police run facial recognition on store footage.

---

5. Important nuance

A few things are often misunderstood:

- Many stores use **face detection** (counting people, demographics) rather than **face identification**.
- Some systems only match against **known offenders**, not everyone.
- A lot of deployments are **small pilots or limited to high-theft stores**.

✅ **Short answer:**
Yes—some retailers (e.g., Macy's, Albertsons, Wegmans, Lowe's, Sainsbury's, Rite Aid) have used facial recognition systems from third-party vendors. In certain cases those vendors operate **shared databases or watchlists** that multiple retailers can access, but many stores keep their own internal lists.

✔ If you want, I can also show you **which companies run the biggest retail facial-recognition databases (and how they actually collect the photos)**—that part is much more surprising.

Sources

-

New York Post

NYC Wegmans storing shoppers' facial scans and biometric data to ID customers, boost security: 'We understand concerns'

January 5, 2026 — Wegmans grocery stores in Brooklyn and Manhattan are now using facial recognition technology to collect and store biometric data—such as facial scans, voiceprints, and eye scans—of customers, which the company says is intended to enhance security. Signs have been posted to notify shoppers, as required by a 2021 NYC law, though enforcement of this law remains weak. Initially piloted in 2024 without data retention, the current system retains facial data until deemed no longer necessary, although specific retention timelines are undisclosed. Wegmans asserts that the technology is used selectively in stores with elevated risk levels and is only employed to identify individuals previously flagged for misconduct, based on police information or internal investigations. The move has sparked privacy concerns, especially amid broader criticism of biometric surveillance. Critics highlight risks including bias, wrongful identification, and data breaches. A City Council bill proposed in 2023 to ban biometric data collection failed, despite notable controversies like facial recognition misuse at Madison Square Garden and Rite Aid's targeting of people of color and women. Wegmans acknowledges these concerns and claims to implement strict training and safeguards, emphasizing that facial recognition is just one part of their investigative process.

Axios

Facial recognition surges in retail stores

July 18, 2021

The Independent

Sainsburys becomes latest to use facial recognition technology inside stores | The Independent

September 1, 2025

Techdirt

Documents Show Clearview Is Selling Facial Recognition Tech To Retailers, Fitness Centers, And Human Rights Violators | Techdirt

February 27, 2020

CNBC

Rite Aid deployed facial recognition in hundreds of U.S. stores

July 27, 2020

American Civil Liberties Union

Are Stores You Shop at Secretly Using Face Recognition on You? | American Civil Liberties Union

March 25, 2018

The Times

Home secretary urges stores to use new crime-reporting platform

July 3, 2025 — The UK government is promoting a new crime-reporting platform, Auror, aimed at tackling rampant shoplifting and antisocial behaviour. Developed by a New Zealand software company, Auror allows major retailers such as Marks & Spencer, Boots, Greggs, Morrisons, BP, and Travis Perkins to share images and details of prolific offenders in a centralized database. Home Secretary Yvette Cooper has urged broader adoption of this system, coinciding with the launch of a three-month "Safer Streets Summer Initiative" involving increased policing in 500 town centres across England and Wales. Auror bridges the gap between retailers and law enforcement by triaging incidents and providing evidence, such as CCTV footage, on prolific offenders to police, which saves resources and increases charge rates. In places like Devon and Cornwall, shoplifting charges have risen by 7% with Auror's support, and reports reach officers 8.5 times faster. While Auror doesn't use live facial recognition, it applies retrospective recognition to link incidents. Cooper also supports broader police use of live CCTV facial recognition, currently used by only two forces. Retail industry studies show 20 million shoplifting offences in the past year, yet only a small percentage are investigated. The system's success in New Zealand and Australia underscores its potential to improve policing efficiency and public safety in the UK.

More

- aclu.org

Retailers Secretively Using Face Recognition to Spot "Persons of Interest" — Including For the Government | American Civil Liberties Union

January 19, 2026 — These are reasonable questions because we know of another corporate mass surveillance system that has definitely been used by the Trump immigration agencies: the driver-surveillance company Flock. Flo...

acs.org.au

Retailers still using facial recognition tech | Information Age | ACS

December 2, 2025 — RETAILERS STILL USING FACIAL RECOGNITION TECH SPARKS WORKPLACE AND CONSUMER RIGHTS CONCERNS. By Jeremy Nadel on Dec 03 2025 05:04 PM Image: Thirsty Camel shopfront One Thirsty Camel manager said...

theguardian.com

Sainsbury’s tests facial recognition technology in effort to tackle shoplifting | J Sainsbury | The Guardian

September 1, 2025 — Image: Customers in a Sainsbury's aisle [Input] The privacy group Big Brother Watch called it ‘chilling’. A similar trial by Asda last year was sharply criticised. Photograph: Bloomberg/Getty Image...

independent.co.uk

Sainsburys becomes latest to use facial recognition technology inside stores | The Independent

September 1, 2025 — MAJOR SUPERMARKET BECOMES LATEST TO USE FACIAL RECOGNITION TECHNOLOGY INSIDE STORES The use of facial recognition at rival supermarket chains have been heavily criticised by privacy groups Henry...

yahoo.com

Sainsbury’s to start using facial recognition technology in shops

September 1, 2025 — SAINSBURY’S TO START USING FACIAL RECOGNITION TECHNOLOGY IN SHOPS * Image: Sainsbury’s to start using facial recognition technology in shops * Image: Sainsbury’s to start using facial recognition te...

cyberlink.com

How Facial Recognition Will Change Smart Retail

May 14, 2025 — HOW FACIAL RECOGNITION WILL CHANGE SMART RETAIL Smart Retail May 15, 2025 "Smart retail" refers to the use of technology in retail environments to enhance the overall shopping experience by improv...

asiaone.com

Australian retail giants named in facial recognition tech complaint, Digital News - AsiaOne

June 27, 2022 — AUSTRALIAN RETAIL GIANTS NAMED IN FACIAL RECOGNITION TECH COMPLAINT Image: Australian retail giants named in facial recognition tech complaint Shoppers walk past stores of Australian electronic goo...

voi.id

Consumer Group In Australia Complains Three Retailers For Using Facial Recognition Technology On Customers

June 26, 2022 — CONSUMER GROUP IN AUSTRALIA COMPLAINS THREE RETAILERS FOR USING FACIAL RECOGNITION TECHNOLOGY ON CUSTOMERS 27 Juni 2022, 16:05 | Editorial Team Major consumer groups have lodged three of Australia'...

silicon.co.uk

Consumer Group Says Major Australian Retailers Using Facial Recognition

June 26, 2022 — CONSUMER GROUP SAYS MAJOR AUSTRALIAN RETAILERS USING FACIAL RECOGNITION Consumer group Choice files with privacy regulator to stop three major Australian retailers from collecting facial recognition...

fightforthefuture.org

24 major U.S. retailers added to the list that’s tracking stores using facial recognition on customers

August 4, 2021 — 24 MAJOR U.S. RETAILERS ADDED TO THE LIST THAT’S TRACKING STORES USING FACIAL RECOGNITION ON CUSTOMERS FOR IMMEDIATE RELEASE: Thursday, August 5 Contact: Caitlin Seeley George, caitlin@fightforthefu...

yahoo.com

The 4 retail stores you probably shop at that use facial-recognition technology

July 18, 2021 — THE 4 RETAIL STORES YOU PROBABLY SHOP AT THAT USE FACIAL-RECOGNITION TECHNOLOGY Hannah Towey Updated Mon, July 19, 2021 at 5:14 PM UTC 3 min read Image * Nonprofit groups are monitoring major re...

wired.com

Some UK Stores Are Using Facial Recognition to Track Shoppers | WIRED

December 19, 2020 — Matt Burgess Business Dec 20, 2020 9:14 AM SOME UK STORES ARE USING FACIAL RECOGNITION TO TRACK SHOPPERS Branches of the British grocer Southern Co-op are using surveillance technology to look fo...

medium.com

Are Stores You Shop at Secretly Using Face Recognition on You? | by ACLU National | ACLU | Medium

March 25, 2018 — And if those things are happening, I think most customers would want to know about it. We don’t know how many of those things are being done by how many American retailers. We do know that the techno...

biometricupdate.com

CSC report finds that 25% of U.K. retailers use facial recognition in store | Biometric Update

September 13, 2015 — CSC REPORT FINDS THAT 25% OF U.K. RETAILERS USE FACIAL RECOGNITION IN STORE Sep 14, 2015, 11:03 am EDT | Justin Lee Categories Biometrics News | Commercial Applications | Facial Recognition...

CR

consumerreports.org

Facial Recognition: Who's Tracking You in Public? - Consumer Reports

FACIAL RECOGNITION: WHO'S TRACKING YOU IN PUBLIC? New technology is moving into the world of department stores, casinos, and cruise ships—and even churches. How freaked out should you be? Image: Co...

NEXT NEW ChatGPT QUERY

ChatGPT query="Where does the feed from USA traffic cameras go and what is it used for?"

In the United States, **traffic camera feeds don't all go to one central place**. They usually go to **several different systems depending on who owns the camera** (city, state, toll authority, or police). The data is then used for multiple purposes.

Here's how it generally works.

---

1. Traffic management centers (most common destination)

Most highway and intersection cameras send their video feed to **regional traffic control centers** run by a state or city transportation agency.

Example systems include programs like Georgia NaviGAtor.

What happens to the feed:

- Cameras send video through fiber or wireless networks to a **Traffic Management Center (TMC)**.
- Operators monitor traffic conditions on large video walls.

- Software may analyze congestion or incidents.

Used for:

- Detecting crashes or stalled vehicles
- Monitoring congestion
- Adjusting variable speed limits or electronic message boards
- Dispatching road service or police
- Managing lane closures or construction

Most of these feeds **aren't permanently stored** or are stored only briefly.

---

2. Public traffic information systems

Some feeds are shared publicly.

They appear on:

- **511 traffic websites**
- TV news traffic reports
- Department of Transportation websites

Example:

- State "511" travel systems
- Live traffic camera maps used by commuters.

Many of these images update every few seconds or minutes and are **open to the public**.

---

3. Automated enforcement systems

Some cameras are used to enforce traffic laws.

These include:

- Speed cameras

- Red-light cameras
- Bus-lane cameras
- Toll-road cameras

The data pipeline is usually:

camera → contractor processing system → law enforcement review → ticket mailed.

What they record:

- Vehicle image
- timestamp
- location
- license plate number

Cities like those running the New York City speed camera program process millions of violations this way each year.

---

4. License plate reader (ALPR) databases

Some roadside cameras automatically read license plates.

These systems are called **ALPR (Automatic License Plate Readers)**.

They are used by police and sometimes private companies such as Flock Safety.

Data collected:

- plate number
- vehicle type/color
- location
- time

The information goes into searchable databases used by police to:

- find stolen vehicles
- locate suspects
- track vehicle movements

Thousands of cities now use these systems.

---

5. Large integrated surveillance systems

In some major cities, traffic cameras feed into broader surveillance platforms.

Example:

- Domain Awareness System

This system integrates:

- CCTV feeds
- license plate readers
- 911 calls
- police reports

Data from cameras may be stored for about **30 days**, while license plate records can be stored for **years**.

---

6. Research and analytics

Universities and transportation researchers sometimes use camera feeds.

They analyze:

- vehicle flow
- pedestrian density
- traffic patterns

Computer vision can convert video into anonymous traffic data such as vehicle speed and trajectories.

✅ Summary

Typical path of a U.S. traffic camera feed:

1. Camera → city/state network
2. Sent to traffic management center
3. Used for:
    - traffic monitoring
    - incident response
    - navigation info
    - ticket enforcement
    - police investigations
    - research/analytics

Different cameras can feed into **different databases simultaneously**.

💡 **Interesting fact:**
The U.S. has **tens of thousands of traffic cameras**, but historically most of the video is only **briefly viewed by operators rather than fully analyzed**, though AI analysis is increasing quickly.

If you want, I can also explain **how police can reconstruct a person's entire driving route using these cameras** (it's surprisingly possible now with modern systems).

Sources

- Argus AI

Traffic Cameras: Untapped Potential for Navigation Routing | Argus AI Blog

December 16, 2024

-

Wikipedia

Traffic camera

-

Wikipedia

New York City speed camera program

-

Wikipedia

Automatic number-plate recognition

-

Wikipedia

Domain Awareness System

-

Department of Transportation

Using Video Feeds from Public Traffic Cameras and Computer Vision to Analyze Social Distancing and Travel Patterns during the COVID-19 Pandemic | US Department of Transportation

July 6, 2021

More

- alibaba.com

Google Maps Traffic Cameras: What They Are & Why They Hurt Tech Efficiency

January 29, 2026 — GOOGLE MAPS TRAFFIC CAMERAS: WHAT THEY ARE & WHY THEY HURT TECH EFFICIENCY 30 January 2026 By Mia Image: Google Maps Traffic Cameras: What They Are & Why They Hurt Tech Efficiency Google Maps traf...

inrix.com

Traffic Cameras | INRIX documentation

October 22, 2025 — TRAFFIC TRAFFIC CAMERAS The INRIX Traffic Camera Service returns data and images about cameras that automatically capture pictures of traffic on major roads. It can be used to find traffic cameras i...

legalclarity.org

Where Are Traffic Cameras Located? How to Find Them - LegalClarity

August 26, 2025 — WHERE ARE TRAFFIC CAMERAS LOCATED? HOW TO FIND THEM Uncover the presence of traffic cameras. Learn how to locate them and understand their various roles on modern roads. LegalClarity Team Publishe...

crockettlawgroup.com

Traffic Camera | Crockett Law Group

July 18, 2024 — TRAFFIC CAMERA Kevin Crockett Managing Partner * July 19, 2024 7 min read 300+ Reviews Traffic cameras are surveillance devices placed at intersections, highways, and busy roads to monitor traf...

trafficcameras.info

About Us - Traffic Cameras

ABOUT US Your Local Traffic Planning Tool Our mission at www.trafficcameras.info is to empower your local journeys by providing you with the most accurate, immediate, and geographically specific tr...

trafficcamarchive.com

TCA | Support & FAQ

▶ Why can I no longer download my videos? Orders expire after 14 days. When an order has expired, the videos are no longer available to download. Contact us if you need assistance. Video ▶ Where d...

trafficvision.live

How to Access Traffic Camera Footage: Request Guide | TrafficVision.Live

HOW TO ACCESS TRAFFIC CAMERA FOOTAGE: REQUEST GUIDE 📌 Table of Contents 7 sections * Can You Access Traffic Camera Footage? * How to Request Traffic Camera Footage * Step-by-Step Process * How to A...

trafficvision.live

Getting Started with Traffic Cameras | TrafficVision.Live

GETTING STARTED WITH TRAFFIC CAMERAS 📌 Table of Contents 14 sections * Why Use Traffic Cameras? * What Cameras Are Available? * Understanding Camera Types * Step 1: Finding Cameras Near You * Step...

What Are Traffic Cameras? (Types, Uses & How to Access Them) | TrafficVision.Live

WHAT ARE TRAFFIC CAMERAS? Types, Uses & How to Access Them 🎥🚗 Traffic cameras are video surveillance systems installed on roads, highways, and intersections to monitor traffic flow and road condit...

seattle.gov

Traffic Safety Camera Program - Transportation | seattle.gov

TRAFFIC SAFETY CAMERA PROGRAM Traffic safety cameras are a proven, effective way to get people to follow traffic laws. This includes stopping at red lights, driving at safe speeds, and following the...

NEXT NEW ChatGPT QUERY

ChatGPT query= “How police can reconstruct a person’s entire driving route using traffic cameras?”

Police can reconstruct a person’s driving route mainly using networks of **traffic cameras and license-plate readers** combined with databases and software that link sightings together. The key technology is called **Automatic Number Plate Recognition (ANPR)** (also called ALPR in the U.S.).

Below is the typical process investigators use.

---

1. Cameras capture license plates automatically

Many road cameras—on traffic lights, highways, toll roads, and police vehicles—are equipped with **ANPR/ALPR** systems.

These cameras:

- Take photos of passing vehicles
- Use **optical character recognition (OCR)** to read the license plate
- Record metadata like:
  - Plate number
  - Date and time
  - Camera location

    - Sometimes vehicle color, make, or model

Infrared lighting often lets them capture plates **day or night**.

Example record stored in a database:

Plate	Time	Location
ABC-123	14:02	Highway exit camera
ABC-123	14:17	Bridge camera
ABC-123	14:34	City intersection

---

2. Each "hit" becomes a timestamped location

Every time your car passes one of these cameras, it generates a **"hit"**.

Police databases may store **millions of these records** from thousands of cameras. For example, some countries run networks capturing **tens of millions of plates per day**.

Each hit is essentially a **GPS-like data point**:

Plate + time + camera location.

---

3. Software links sightings into a route

Investigators query the database for a specific license plate.

The system returns all sightings of that vehicle:

```
Camera A – 08:11
Camera B – 08:26
Camera C – 08:41
Camera D – 09:03
```

From this, software can reconstruct:

- Travel direction
- Approximate route
- Travel speed

- Stops or detours

This is sometimes called building a **"pattern of life"** for the vehicle.

---

4. Multiple camera networks are combined

Police often combine data from many sources:

- City traffic cameras
- Highway cameras
- Toll-road systems
- Parking garage cameras
- Private camera networks (e.g., neighborhood systems)
- Police vehicle ALPR cameras

Some surveillance platforms even integrate **tens of thousands of cameras and billions of license-plate records** for search and analysis.

---

5. AI can track vehicles even without the plate

If the plate is unreadable or missing, systems can still track cars using **visual fingerprints**, such as:

- Vehicle color
- Make and model
- Damage, decals, or roof racks
- Unique shape or features

Some systems call this **"vehicle fingerprint technology."**

---

6. Investigators can work backwards

If a crime happens at 10:00 PM:

1. Police search for vehicles seen near the crime scene.
2. They find the suspect car.

3. They query earlier camera hits of that plate.
4. The database reconstructs where the car came from and where it went afterward.

✅ **In simple terms:**
Police rebuild a driving route by **connecting many camera sightings of the same license plate across a city or highway network**, producing a timeline of locations.

💡 If you want, I can also explain:

- How accurate these systems are (and their failure rates)
- How investigators track cars **even if the plate is covered or changed**
- Or how dense camera networks in major cities can track almost every trip.

“How police can reconstruct a person’s entire driving route using traffic cameras?”

Sources

W

Wikipedia

Automatic number-plate recognition

WTAE

Border Patrol uses license plate readers nationwide to flag suspicious drivers

November 19, 2025

Domain Awareness System

Flock Safety

More

paloalto.gov

Automated License Plate Recognition (ALPR) – City of Palo Alto, CA

February 3, 2026 — AUTOMATED LICENSE PLATE RECOGNITION (ALPR) Image The Palo Alto Police Department uses automated license plate recognition (ALPR) technology to deter criminal activity and assist in criminal investi...

crown.edu

License Plate Recognition: How It Works

January 5, 2026 — The camera’s placement is also super important. They need to be positioned at just the right angle and distance to get a good shot of the plate. Sometimes, you’ll see multiple cameras working together...

yahoo.com

‘Creeped out’ or crime solvers? License plate readers stir debate

December 26, 2025 — HOW IT WORKS The software on the cameras compares a license plate number against different national crime databases, including an Amber Alert database and the National Crime Information Center databa...

kcra.com

Border Patrol uses license plate readers nationwide to flag suspicious drivers

November 19, 2025 — The chats show how thoroughly Texas highways are surveilled by this federal-local partnership and how much detailed information is informally shared.In one exchange a law enforcement official included...

yahoo.com

Police Used Flock Cameras To Track One Driver Over 500 Times. Now They're Being Sued

October 3, 2025 — POLICE USED FLOCK CAMERAS TO TRACK ONE DRIVER OVER 500 TIMES. NOW THEY'RE BEING SUED Paul Stadden Sat, October 4, 2025 at 10:05 PM UTC 5 min read Image: A white traffic camera mounted on an orang...

flocksafety.com

Security Strategies From Law Enforcement Investigators Part 3: Connecting Crime Across Multiple Locations with License Plate Reader Cameras

June 26, 2025 — SECURITY STRATEGIES FROM LAW ENFORCEMENT INVESTIGATORS PART 3: CONNECTING CRIME ACROSS MULTIPLE LOCATIONS WITH LICENSE PLATE READER CAMERAS Learn how businesses can use license plate reader cameras...

ecam.com

License Plate Recognition: Everything You Need to Know | ECAM

April 13, 2025 — WHAT IS LICENSE PLATE RECOGNITION TECHNOLOGY? Like any technology, some work better than others. Automated license plate readers contain high-speed, IP camera systems that companies can mount almost...

congress.gov

August 18, 2024 — Law Enforcement and Technology: Use of Automated License Plate Readers August 19, 2024 (R48160) Jump to Main Text of Report CONTENTS * ALPRs and How They Work * How LPRs May Be Used by Law Enforcem...

police1.com

3 scenarios where advanced LPR capabilities shine

December 21, 2021 — 3 SCENARIOS WHERE ADVANCED LPR CAPABILITIES SHINE THE FEATURES PROVIDED BY ADVANCED LICENSE PLATE RECOGNITION PROVIDE LAW ENFORCEMENT WITH A RANGE OF TACTICAL AND INVESTIGATORY ADVANTAGES December...

trea.com

METHOD AND APPARATUS FOR TRAFFIC INFRACTION MANAGEMENT | TREA

March 3, 2021 — For purposes of discussion, we will refer to the image capture device 102 as a smartphone. It should be noted that the system may be implemented with a variety of standalone and integrated image captu...

police1.com

How to take the guesswork out of license plate identification

February 16, 2021 — HOW TO TAKE THE GUESSWORK OUT OF LICENSE PLATE IDENTIFICATION OPTICAL CHARACTER RECOGNITION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE LEAD TO MORE ACCURATE LICENSE PLATE READINGS February 17, 2021 12:...

claytonrice.com

Automated Licence Plate Readers | Clayton Rice, K.C.

September 14, 2020 — AUTOMATED LICENCE PLATE READERS * September 15, 2020 * Clayton Rice, K.C. An automated licence plate reader combines a high-speed camera with image-processing technology to capture licence plate nu...

police1.com

Police implementation of an ALPR system

June 26, 2018 — 8 STEPS TO SUCCESSFUL IMPLEMENTATION OF AN ALPR SYSTEM CREATING AND USING ALPR IS NO LONGER IN THE CATEGORY OF INNOVATIVE POLICING – IT IS AN ESSENTIAL TOOL FOR EFFECTIVE LAW ENFORCEMENT June 27, 2...

wired.com

License to Spy | WIRED

November 30, 2014 — The Obama administration is attempting to get a better understanding of LPR use. In May, the Department of Justice created a task force to study guidelines for law enforcement, and in September, the U...

notrace.how

You Can't Catch What You Can't See: Against Video Surveillance | No Trace Project

AUTOMATIC LICENCE PLATE RECOGNITION (ALPR) This technology identifies vehicle licence plates using optical character recognition. To film licence plates at night, the cameras emit infrared light. The...

theiacp.org

Automated License Plate Recognition | International Association of Chiefs of Police

RESEARCH & REPORTS Jurisdictions throughout the nation and around the world are continuing research on current operations, emerging best practices, performance metrics, and business benefit realizati...

jenoptik.us

Identify, monitor and intercept suspect vehicles | Jenoptik USA

* ## Monitoring suspect vehicles with ALPR Record the license plates of suspect vehicles and analyse their movements. Use the data to create criminal profiles and movement patterns. RecommendFacebo...

jenoptik.us

Combat crime with ALPR cameras | Jenoptik USA

COMBAT CRIME WITH ALPR CAMERAS Record and evaluate ALPR data in real time by using VECTOR³ cameras, TraffiData analysis software and TraffiMobile® cameras for combating crime. Jenoptik's advanced t...

sztigerwong.com

Case Studies: Successful Implementations of ALPR Camera Systems - Tigerwong Parking

Success Story 1: Denver Police Department Denver Police Department The Denver Police Department (DPD) implemented an ALPR camera system in their patrol cars to aid in criminal investigations and tr...

sighthound.com

How ALPR Works: A Deep Dive into Parking & Patrol Systems | Sighthound

HOW ALPR WORKS (WITH EXAMPLES FROM REAL PARKING LOTS & PATROL CARS) Jan 29 Written By Ali Ahad It happens in the blink of an eye, literally. A vehicle approaches a corporate parking barrier at 15...

sciencedirect.com

Detection and tracking strategy for license plate detection in video - ScienceDirect

OPTIK Volume 125, Issue 10, May 2014, Pages 2283-2288 DETECTION AND TRACKING STRATEGY FOR LICENSE PLATE DETECTION IN VIDEO https://doi.org/10.1016/j.ijleo.2013.10.126Get rights and content ABSTRA...

NEXT NEW ChatGPT QUERY

ChatGPT query="How long is license-plate info from traffic cameras data typically stored in the USA?"

The retention time for **license-plate data from traffic or surveillance cameras** (often called **ANPR/ALPR — Automatic Number Plate/License Plate Recognition**) varies widely by **country, agency, and camera type**. But there are some common ranges.

Typical retention ranges

Across many jurisdictions, **plate-scan data is usually kept anywhere from a few days to about a year**.

- **7–30 days** – common for many **city or private camera networks** (especially commercial systems or pilot programs).
- **30–90 days** – common for **local police databases** or systems meant for short-term investigations.
- **6–12 months** – common for **national or large police databases**.
- **Multiple years or indefinite** – sometimes occurs when the data is copied into larger investigative systems or kept for ongoing cases.

Example policies:

The length of time that license plate information from traffic cameras is stored in the USA varies significantly depending on the jurisdiction, agency policies, and the specific purpose for collecting the data. However, there are some general guidelines:

1. State and Local Regulations:

- **Short-Term Storage**: In many places, license plate data collected by traffic cameras is stored for **30 to 90 days**. This is typically the case for data used in routine traffic enforcement or surveillance. It may be kept for a few weeks or months to help with investigations or violations.
- **Long-Term Storage**: In some regions, particularly for systems that are integrated with broader law enforcement databases (like

the **ALPR** or Automated License Plate Recognition systems), the data might be stored for a **year or longer**. This allows law enforcement to look back at historical data for investigations, especially if the data has been linked with crimes or ongoing investigations.

2. Data Retention Policies:

- Some cities or counties have clear public policies about data retention, requiring the deletion of license plate information after a certain period to protect privacy. In other cases, data might be stored indefinitely unless requested for deletion by citizens or based on specific legal requests.

- For example, **California** has laws that limit how long law enforcement can retain license plate data from ALPR systems. Under **California law (California Government Code 6254.24)**, data should be deleted within **60 days** unless it is part of an investigation or legal case.

3. Federal Guidelines:

- While there is no universal federal law specifying retention periods for license plate data, federal agencies like the **Department of Homeland Security (DHS)** and **FBI** can access ALPR data stored by state or local agencies, depending on the specific system and collaboration agreements.

- Additionally, if the data is used for broader surveillance (e.g., tracking movements across state lines), the storage period can extend longer based on the specific program.

4. Private Systems:

- In cases where private companies operate traffic cameras, such as those used for toll collection or private security, data retention periods can vary even more. Some private systems might only keep the data for a short time for billing or security purposes, while others could retain it for months or even years.

In Summary:

- License plate data is typically stored for **30 to 90 days** but can be retained **longer (1 year or more)**, especially if linked to investigations.
- Retention policies depend on **local laws**, **state regulations**, and the **purpose** for data collection (e.g., law enforcement, tolling, or surveillance).
- Some jurisdictions, like **California**, have specific laws that govern retention periods and deletion of this data.

If you want more specific info for a particular city or state, I can try to find that for you!

Some commercial networks used by police departments store plate data **about 30 days by default**.

What exactly gets stored

A typical camera capture record includes:

- License plate number
- Timestamp
- GPS/location of the camera
- One or more photos of the vehicle (sometimes including occupants)

These records allow investigators to **reconstruct a vehicle's past movements** if the data is still within the retention window.

Important nuance

Retention depends heavily on **why the camera exists**:

- **Speed cameras / toll systems:** often keep images **until the ticket process is complete**, then delete them.
- **Police ANPR networks:** usually keep data **months to a year** for investigative searches.

- **Private neighborhood or retail cameras:** often keep data **7–30 days** unless flagged.

Also, if a plate is linked to an investigation, the record can be **preserved indefinitely as evidence**.

✅ **Bottom line:**
Most traffic-camera license-plate data is typically stored **between 30 days and 12 months**, but policies vary widely and some systems retain it much longer.

If you want, I can also explain **how easy it is for police to reconstruct a car's past routes from these databases** (it's more powerful than most people realize).

NEXT NEW ChatGPT QUERY

ChatGPT query= "How do criminals sometimes try to evade traffic camera tracking?"

Some criminals **attempt** to avoid or confuse traffic-camera systems, but it's important to note that these actions are illegal in many places and law-enforcement agencies continually improve technology to detect them. 🚗📷 I can describe the **general categories** of tactics people have tried and how authorities counter them—without going into operational details.

1. Obscuring or altering vehicle identification

Some offenders try to make their vehicle harder to identify in images captured by **automatic license-plate readers** (ALPR systems). In general terms, this can involve attempts to hide, distort, or temporarily change identifying features of a vehicle.

Countermeasures:

- Cameras capture multiple angles and high-resolution images.
- Police cross-reference vehicle make, color, stickers, damage patterns, and timestamps.

- Tampering with plates is usually a separate criminal offense.

2. Switching vehicles

In organized crimes, offenders sometimes **switch to different vehicles** during or after an incident to break the visual trail that cameras might follow.

Countermeasures:

- Investigators analyze camera networks across multiple streets.
- They use time-sequence tracking to reconstruct travel routes and find transfer points.

3. Route manipulation

Some individuals attempt to **avoid known camera locations** by choosing alternative streets.

Countermeasures:

- Many cities have **dense camera networks**, including private cameras from businesses and residences.
- Investigators also combine traffic footage with toll systems, parking records, and other digital traces.

4. Use of stolen or cloned plates

In some cases, criminals use **plates not registered to the vehicle** they're driving.

Countermeasures:

- Systems compare the plate number with the vehicle's expected make/model/color.
- Mismatches trigger alerts for investigation.

5. Timing or environmental tricks

People have occasionally tried to exploit darkness, weather, or glare to reduce image clarity.

Countermeasures:

- Modern cameras use infrared illumination, high dynamic range sensors, and AI-assisted recognition that works in poor lighting.

✅ **Key point:** Even when someone tries these tactics, investigators usually combine **multiple data sources** (camera networks, GPS/toll data, witness footage, and forensic analysis). As a result, attempts to evade traffic cameras often **fail and add extra charges**.

If you want, I can also explain **how traffic camera systems and license-plate recognition actually work** behind the scenes.

NEXT NEW ChatGPT QUERY

ChatGPT query= "Are traffic cameras in squad cars a continuous live feed into ALPR/ANPR systems regardless of whether the squad is in motion or the driver is out of the vehicle?"

Short answer: **Usually yes, but it depends on the system and department configuration.** Most modern patrol cars equipped with **ALPR/ANPR (Automatic/Automated License Plate Recognition)** can scan plates **continuously whenever the system is powered on**, whether the vehicle is moving or parked. However, the **live feed behavior and data transmission** varies by vendor, policy, and connectivity.

How ALPR Cameras in Patrol Cars Typically Work

1. Continuous plate scanning

Modern mobile ALPR systems (from companies like Flock Safety, Motorola Solutions, or Vigilant Solutions) usually run **continuously when active**:

- Cameras mounted on the **roof, light bar, trunk, or rear window**
- They capture images of passing vehicles' plates
- Software converts them into plate numbers using OCR

- Plates are compared against **hotlists** (stolen cars, warrants, Amber alerts)

This works **whether the patrol car is:**

- Driving
- Parked on the roadside
- Parked while the officer is outside the vehicle

The cameras simply keep scanning whatever enters their field of view.

---

2. Real-time alerts vs stored scans

There are two common operating modes:

Real-time local processing

- The in-car computer processes plates instantly
- If a plate matches a hotlist → the officer gets an alert

Cloud/networked systems

- The plate image and metadata (time/location) may be uploaded to a central server
- Other agencies can query it later

Continuous scanning does **not necessarily mean continuous live streaming to a central database**; sometimes it **buffers locally and uploads later**.

---

3. Motion is not required

Mobile ALPR cameras are specifically designed to read plates:

- **While both vehicles are moving**
- **While only one vehicle is moving**
- **When the patrol car is stationary**

So an officer could park on a street or in a parking lot and the system will still scan passing plates.

---

4. When scanning might stop

Scanning can stop if:

- The officer **turns off the ALPR system**
- The vehicle **power is off**
- Department policy requires **manual activation**
- Cameras are **linked to ignition state**
- The network connection drops (though scanning may still occur locally)

Some departments require the system to be **manually enabled during patrol shifts**.

Important distinction: dash cameras vs ALPR cameras

- **Dash cams:** record video for evidence (may or may not run continuously)
- **ALPR cameras:** specialized cameras optimized for **plate detection**, often with infrared illumination.

They are usually **separate systems**, even though they may be mounted near each other.

✅ **Typical patrol setup:**

- 2–4 ALPR cameras on the light bar or trunk
- Continuous scanning while powered
- Instant alerts if a plate matches a database

💡 **Interesting detail:**

A single patrol car with ALPR can scan **thousands of plates per shift**, even

while parked.

If you want, I can also explain:

- **How accurate ALPR actually is (and when it fails)**
- **How long police databases typically store plate scans**
- **How many plates a patrol car can realistically read per minute** (the numbers are surprising).

NEXT NEW ChatGPT QUERY

ChatGPT query= “Are USA traffic camera feeds ever used for facial recognition?”

Short answer:
Generally **no—typical U.S. traffic cameras are not used for facial recognition.** Most systems are designed to identify **vehicles (especially license plates)** rather than the people inside them. However, there are **some exceptions involving other surveillance cameras**, and the overall ecosystem can still intersect with facial recognition in certain investigations.

---

1) What most U.S. traffic cameras actually do

Most roadside enforcement cameras use **Automatic License Plate Recognition (ALPR)** or similar systems.

- They capture a photo of a passing vehicle.
- Software reads the **license plate number** and logs **time, date, and location**.
- The plate can be checked against databases (stolen cars, AMBER alerts, etc.).

Important:

- These systems are **designed to identify vehicles, not drivers or passengers**.
- Many implementations explicitly **do not use facial recognition**.

Typical examples:

- **Red-light cameras**
- **Speed cameras**
- **ALPR road cameras used by police**

Some traffic programs even intentionally avoid photographing the driver to reduce privacy issues; for example, certain red-light camera programs issue tickets to the **vehicle owner**, not a specific driver.

---

2) Why facial recognition usually isn't used

There are practical and legal reasons:

Technical limitations

- Cameras are positioned to capture plates or vehicle rear views.
- Drivers' faces are often obscured by angle, glare, or movement.

Legal/privacy concerns

- Many states restrict biometric surveillance.
- Facial recognition in policing has been controversial and regulated in some cities.

---

3) Where facial recognition *does* show up

Facial recognition **is used in U.S. policing**, but usually in **other camera networks**, not standard traffic cameras.

Examples include:

- City surveillance cameras
- CCTV systems around public spaces
- Security cameras at businesses or transit hubs

Police may run facial recognition **after a crime**, comparing images from cameras to databases of known individuals. Some cities have used large camera networks for this kind of investigation.

There have also been controversial cases where camera networks (not typical traffic cameras) were used for **real-time facial recognition alerts**, sparking legal debates.

✅ **Bottom line:**

- **Normal traffic enforcement cameras in the U.S. → usually read license plates only.**
- **Facial recognition → used mainly with other surveillance cameras**, sometimes later during criminal investigations.

💡 If you want, I can also explain something many people find surprising: **how police can sometimes identify a person from traffic cameras even without facial recognition** (there are a few indirect methods).

NEXT NEW ChatGPT QUERY

ChatGPT query= “How police can sometimes identify a person from traffic cameras even without facial recognition.”

NEXT NEW ChatGPT QUERY

ChatGPT query= “How to detect which USA traffic camera feeds are for automated ticketing?”

In the U.S., **not every traffic camera issues tickets**. Many are only for **traffic monitoring** (run by state DOTs), while **automated enforcement cameras** are used specifically for violations like red-light running or speeding. Here are the practical ways to tell which ones are used for ticketing.

---

1. Check if the camera is part of an automated enforcement program

Only cameras in official **red-light or speed camera programs** issue tickets. These programs are run by cities/counties and usually listed publicly.

Examples:

- New York City Department of Transportation — publishes locations for its speed cameras.
- Chicago Department of Transportation — lists red-light and speed camera intersections.
- Los Angeles Department of Transportation — previously ran red-light cameras (most now inactive).

Tip: Search:
`<city name> red light camera locations` or `<city> automated speed enforcement`.

If a camera is **not on an official list**, it usually **cannot issue tickets**.

---

2. Look for warning signs near the intersection

Most states legally require signage before automated enforcement.

Typical signs:

- "**Photo Enforced**"
- "**Red Light Photo Enforcement**"
- "**Speed Safety Camera Ahead**"

If there is **no warning sign**, it's often just a **traffic monitoring camera**.

---

3. Identify the camera hardware type

Automated ticket cameras have specific hardware.

Common systems include:

- Verra Mobility (formerly American Traffic Solutions)
- Redflex Traffic Systems
- Sensys Gatso Group

Characteristics:

- Mounted on **intersection poles or arms**
- Often **multiple cameras** aimed at lanes
- **Flash units or radar boxes**
- **Ground sensors or radar units**

Traffic monitoring cameras (DOT cameras) usually:

- Are **single PTZ cameras**
- Mounted high on **freeway poles**
- **No flash or radar hardware**

---

4. Check the feed owner

Most **public livestream traffic cameras** come from state DOT systems like:

- California Department of Transportation
- Texas Department of Transportation
- Florida Department of Transportation

These **do not issue tickets** — they're just for congestion monitoring.

Automated enforcement cameras **rarely publish live feeds** because they capture license plates for enforcement.

---

5. Use enforcement camera databases

These sites map known ticket cameras:

- Waze (community-reported speed/red-light cameras)
- OpenStreetMap tags: `highway=speed_camera`
- PhotoEnforced.com database of US enforcement cameras

---

6. State legality matters

Many states **ban automated ticketing** entirely. For example:

- Banned: Texas (red-light cameras banned in 2019)
- Mostly banned: Mississippi
- Limited use: California (red-light only in some cities)

If the state bans them, **no camera feed there can issue tickets**.

✅ Quick rule of thumb

Camera type	Tickets?
State DOT highway camera	❌ No
City intersection with “Photo Enforced” sign	✅ Yes
Livestream traffic cam website	❌ No
Hidden camera with flash/radar box	Usually yes

Important: If you’re analyzing **public camera feeds**, almost none of those are used for ticketing because automated enforcement systems **don’t provide public livestreams**.

If you want, I can also show you:

- **How to programmatically identify enforcement cameras from open data or map data**

- **Which US states/cities actually publish enforcement camera datasets**
- **How researchers detect ticket cameras using computer vision from street images**.

NEXT NEW ChatGPT QUERY

ChatGPT query= “What is the position of hidden cameras in modern cars”
Modern cars often come equipped with a variety of cameras, both visible and hidden, to enhance safety, security, and driver convenience. Hidden cameras in particular are typically used for surveillance, driver monitoring, or security features. Here are some common positions where hidden cameras might be located in modern cars:

1. Rearview Mirror (Driver Monitoring)

- **Purpose:** Used for monitoring the driver’s attention and facial expressions (part of advanced driver assistance systems, or ADAS). This camera can help detect drowsiness, distraction, or even changes in the driver’s gaze.
- **Location:** Typically housed in or near the rearview mirror assembly. It’s often a small, unobtrusive camera.

2. Dashboard (Interior Surveillance)

- **Purpose:** Hidden cameras might be used for interior surveillance, either for monitoring passengers or providing security footage (for example, in case of theft or accidents).
- **Location:** Embedded in the dashboard, often around the central infotainment area or near the glove compartment. Some systems also use a combination of cameras for monitoring all angles of the car interior.

3. Side Mirrors (Side View Cameras)

- **Purpose:** Not exactly hidden, but small cameras mounted in side mirrors or mirror housings can provide a "blind spot" view to

help drivers during lane changes. These cameras might also serve as part of a broader surveillance system.

- **Location:** Integrated into the side mirrors, often behind the mirror glass or within the housing itself.

4. License Plate Area (Security)

- **Purpose:** Some vehicles are equipped with cameras near the license plate area to monitor activity around the car when parked (for security purposes, or as part of parking surveillance systems).
- **Location:** The cameras may be hidden inside the license plate frame or the bumper area.

5. Front Bumper (Parking Assist)

- **Purpose:** Cameras in this area help with parking assistance and offer a view of obstacles ahead of the car. These can also be part of an integrated surveillance system in some cases.
- **Location:** Typically hidden behind the front bumper or grill.

6. Car Trunk (Cargo Surveillance)

- **Purpose:** In some high-end vehicles or for fleet security, cameras may be hidden in the trunk to monitor what is being stored or to track items being loaded or unloaded.
- **Location:** Inside the trunk, typically near the trunk latch or high up on the rear shelf area.

7. A-Pillars and C-Pillars (Blind Spot Monitoring)

- **Purpose:** Small, discreet cameras can be mounted to assist with blind-spot detection or monitoring the surrounding environment of the car.
- **Location:** The A-pillar (the vertical supports on either side of the windshield) or the C-pillar (near the rear window or door).

8. Rear Seats (Passenger Surveillance)

- **Purpose:** In some cases, hidden cameras may be placed in the rear seat area for monitoring passengers, such as in commercial vehicles (e.g., taxis, ride-sharing cars) or as part of a fleet management system.
- **Location:** Hidden within the ceiling, headrests, or along the interior trim of the car.

9. Under the Vehicle (Vehicle Surveillance)

- **Purpose:** Some vehicles may have cameras or sensors installed under the car, primarily for monitoring obstacles or for advanced parking assistance features.
- **Location:** Hidden underneath the vehicle, often integrated into the undercarriage or suspension components.

10. Inside the Sunroof (Optional Interior Monitoring)

- **Purpose:** Some luxury or high-tech vehicles use cameras inside the sunroof area to help monitor passengers or record their actions (often used for advanced in-car entertainment or interaction features).
- **Location:** Hidden within the sunroof's frame or area surrounding the sunroof.

Key Uses of Hidden Cameras in Modern Cars:

- **Driver Assistance & Safety:** Cameras for lane-keeping, collision avoidance, adaptive cruise control, and driver alertness.
- **Surveillance & Security:** Cameras that monitor passengers, the interior, or the perimeter of the vehicle when parked.
- **Parking & Maneuvering:** Cameras embedded in bumpers or mirrors to assist with parking, reversing, and detecting nearby obstacles.

In all cases, the exact design and placement will vary depending on the vehicle's brand, model, and specific features.

NEXT NEW ChatGPT QUERY

ChatGPT query="What is the position of hidden microphones in modern cars"
The position of hidden microphones in modern cars is often strategically chosen to serve various functions, such as enabling hands-free calling, voice commands, or advanced driver assistance systems (ADAS). While car manufacturers might not disclose the exact locations of these microphones, here are some common areas where they are typically found:

1. **Rearview Mirror**:
   This is one of the most common spots for hidden microphones. Positioned in the center of the cabin, it provides an optimal location for picking up clear voice signals from the driver and passengers. Additionally, it works well for hands-free communication or voice-activated systems, as it minimizes noise from outside the vehicle.

2. **Headliner (Ceiling)**:
   Microphones may be mounted in the headliner, usually near the front cabin area or along the sides. This helps capture voices without interference from the vehicle's air conditioning or engine noise. In higher-end vehicles, microphones may be integrated into the headliner near the driver's seat or center console.

3. **A-Pillar**:
   Some manufacturers place microphones in or near the A-pillars (the columns on either side of the windshield) to capture sound from both the driver and front passenger. This placement is useful for voice recognition systems, as the microphones can isolate the sound from inside the car.

4. **B-Pillar**:
   For larger vehicles, such as SUVs or minivans, microphones

may be located along the B-pillar (the vertical support between the front and rear doors). This is particularly useful for capturing clear speech from rear-seat passengers for voice-controlled systems.

5. **Dashboard or Console**:
   Some modern cars have small microphones embedded in the dashboard or central console. These might be part of the infotainment system, allowing drivers to make voice commands or take calls.

6. **Near the Seatbelt or Headrests**:
   In certain cases, microphones are located near the headrests or integrated into the seatbelt system to improve sound quality for conversations happening within the cabin. This also helps with isolating the driver's voice from ambient noise.

These microphones are usually used for **in-car communication**, **voice recognition**, and **infotainment systems**. Additionally, some newer models use multiple microphones for **noise cancellation** or **sound enhancement**.

There are also **privacy concerns** related to the hidden microphones, especially when connected to cloud-based services that could theoretically record and transmit data. However, most manufacturers implement strict privacy protocols to address these issues.

Are you thinking about a specific car brand or model? Or is this related to a particular concern or interest?

NEXT NEW ChatGPT QUERY

ChatGPT query= "What are modern cars recording surveillance systems"

Modern cars *aren't just vehicles anymore* — many now include multiple systems that continuously **record video, sensor data, and other information** for safety, navigation, automation, and security purposes. These systems can act like onboard surveillance both **inside and outside the vehicle**.

📸 1. Built-in Cameras & Dashcams

Many new cars include or **offer factory-integrated cameras** that can record video of the road, surroundings, and sometimes the interior:

Dashcams: Originally aftermarket devices, dashcams now are sometimes **factory-installed** and record front (and sometimes rear) views of the road. They continuously buffer video and save clips when triggered by events like collisions.

Parking surveillance systems: Systems like Tesla's *Sentry Mode* use the car's external cameras to watch for suspicious motion while parked and save video if triggered.

360° systems: Some luxury brands bundle front, rear, and side cameras into a 360° recording/monitoring setup to help with parking and security.

🧠 2. Event Data Recorders ("Black Boxes")

Almost all modern vehicles include an **Event Data Recorder (EDR)** — similar to an airplane's black box — that continuously logs data such as:

- vehicle speed
- braking and acceleration
- steering input
- sensor status before, during, and after a crash.

EDRs don't typically store full video — they log numerical data and are designed primarily for crash analysis.

📡 3. Telematics & Video Telematics

Many cars combine cameras with **telematics systems** — communications systems that transmit data over cellular or Wi-Fi networks:

- GPS location, speed, and routes
- collision and vehicle health data
- video clips in vehicle fleets for safety monitoring

Such systems can upload footage and sensor data to cloud servers for later review.

🧠 4. Driver Monitoring & Interior Recording

A growing number of vehicles now have **inside-facing cameras** intended to monitor driver attention and safety (e.g., eye gaze, distraction) or for advanced autonomous features.

Some high-end cars also use interior cameras for security or driver recognition.

📊 5. Other Data Collected

Beyond video, cars collect a wide range of data that might be shared with manufacturers or third parties:

- GPS location and trip history
- Bluetooth and infotainment synced data
- acceleration, brake patterns, steering data
- Safety system performance and warnings

🔒 Privacy & Legal Aspects

Privacy Risks

As cars collect more data, **privacy concerns** have increased:

- footage and sensor data can be transmitted off the vehicle.

law enforcement has, in some cases, sought access to footage from parked vehicles with surveillance modes.

- manufacturer data collection practices vary and are often controlled by complex privacy agreements.

Legal Regulations

- Dashcam use and data protection are regulated differently by country — some nations restrict continuous public surveillance.

🧭 In Summary

Modern cars increasingly function as **smart, connected recording devices**:
✅ External dashcams and parking cameras capture video of the road and surroundings.
✅ EDRs log detailed numeric data around collisions.
✅ Telematics can transmit data to manufacturers or cloud services.
✅ Interior cameras and sensors monitor driver behavior.
All of this can help safety and diagnostics — but it also means cars collect and sometimes share detailed data about your driving and environment.

If you want, I can go deeper into **specific brands and models that include these systems** or how to manage your **privacy settings** in modern cars.

NEXT NEW ChatGPT QUERY

ChatGPT query= “Is there an industry standard AV format for the footage taken by secret cameras in modern cars?”

There is **no single universal “industry standard” format mandated for car security/dash cameras**, but in practice almost all modern vehicle camera systems converge on the same **two-layer structure**:

1. **Container format:** usually **MP4**
2. **Video codec: H.264 (AVC)** or **H.265 (HEVC)**

1. Container format (file wrapper)

Most automotive camera systems save clips in **MP4 file format** (`.mp4`). This container can hold compressed video, audio, timestamps, and metadata, which makes it widely compatible with players and editing tools.

Some manufacturers use alternatives like `.mov`, `.ts`, or proprietary wrappers, but they are less common.

2. Video codec (actual compression)

The video inside the file is typically encoded with one of these codecs:

- **H.264**

- Historically the most common video compression standard.
- Used in most dashcams and early automotive recording systems.
- Widely supported on computers and phones.

H.265

- Newer and more efficient (better quality at lower bitrates).
- Increasingly used in newer dashcams and car security systems.

3. Typical setup in modern cars

A typical modern vehicle security recording stack looks like:

```
Container: MP4
Codec:     H.264 or H.265
Resolution: 1080p–4K
Frame rate: 30–60 fps
Storage:   SD card or USB drive
Segmented files: 1–5 minute clips
```

Many systems also store **metadata alongside the video**, such as:

- GPS coordinates
- timestamp
- vehicle speed
- camera ID (front/rear/side)
- event markers (collision, motion detection)

These may appear in **JSON, CSV, or embedded MP4 metadata tracks**.

4. "Secret cameras" specifically

For **covert or security cameras integrated by OEMs** (parking surveillance, driver monitoring, etc.):

- The **codec/container is still usually MP4 + H.264/H.265**.

- But the **file structure and metadata are often proprietary** (e.g., multi-camera sync files, encrypted storage).

Examples include:

- parking surveillance systems
- interior driver-monitoring cameras
- fleet telematics cameras

5. Why this combination dominates

Automotive systems prefer **MP4 + H.264/H.265** because it:

- minimizes storage usage (cars record continuously)
- is hardware-accelerated in embedded chips
- works across almost all devices for evidence review
- supports high-resolution multi-camera setups

✅ **Short answer:**
The closest thing to an industry default for vehicle security footage today is **MP4 container with H.264 or H.265 video encoding**.

If you want, I can also explain **how multi-camera cars (like Teslas or ADAS systems) structure their footage**, which is quite interesting because they often synchronize **4–8 cameras at once**.

**

NEXT NEW ChatGPT QUERY

ChatGPT query= “How do police or manufacturers sometimes extract hidden pre-crash video buffers, and which brands actually store the most camera footage?”

NEXT NEW ChatGPT QUERY

ChatGPT query= “Is retrieval of the footage taken by secret cameras in modern cars always done by the dealer and is it logged?”

No—**retrieving footage from cameras in modern cars is not always done by the dealer, and it is not always logged.** It depends heavily on the **vehicle brand, camera type, and where the footage is stored.** 🚗📹

Here are the main cases:

---

1. Built-in dashcam systems (owner-accessible)

Many newer cars have integrated dashcams where **the owner retrieves the footage directly**, usually via:

- USB drive or SD card
- Mobile app
- Infotainment system export

Examples:

- Tesla Model 3 / Tesla Model Y with **Tesla Dashcam and Sentry Mode**
- BMW 5 Series with **Drive Recorder**
- Mercedes-Benz S-Class with **Dashcam feature**

In these systems:

- The **driver/owner usually retrieves footage**
- **Dealers are not involved**
- Logging varies (some systems log when clips are exported)

---

2. ADAS / safety camera data (usually not normal "video footage")

Many cars have cameras used for driver assistance systems like:

- Lane keeping
- Collision avoidance
- Parking assist

Examples of brands with extensive camera systems:

- Toyota
- General Motors
- Ford Motor Company

These cameras typically:

- **Do not store continuous video**
- Store **short event buffers** (seconds before/after a crash)
- Are mainly used for **diagnostics or crash investigation**

Retrieval may require:

- manufacturer diagnostic tools
- sometimes **dealer or manufacturer access**

Logging:

- Often **yes** in diagnostic logs, but not always visible to the owner.

---

3. Event Data Recorders (EDR / "black boxes")

Most modern cars sold in the U.S. have an **Event Data Recorder** mandated by regulations from the National Highway Traffic Safety Administration.

However:

- **EDRs usually record sensor data**, not video

- Data extraction typically requires **special tools**
- Access is usually by:
  - investigators
  - insurers
  - repair technicians

Some vehicles require a **dealer or manufacturer interface**, but independent investigators can also retrieve it.

Logging:

- Access may be logged in **diagnostic systems**, but not universally.

---

4. Cloud-connected vehicles

Some brands upload data to cloud services, such as:

- Tesla
- General Motors (via OnStar)
- BMW ConnectedDrive

Possible characteristics:

- Clips or event snapshots **may be uploaded**
- Retrieval may occur via **apps, manufacturer portals, or internal systems**
- Access **may or may not be logged**, depending on the backend system.

✅ Summary

Question	Reality
Is footage always retrieved by the dealer?	❌ No — often the owner can retrieve it

Is retrieval always logged?	❌ Not guaranteed
Do all car cameras record video?	❌ Many only process images in real time
Can others retrieve it?	Sometimes (investigators, insurers, manufacturer tools)

Important: Many cars have cameras that **never store footage at all**—they only process images temporarily for driving assistance and then discard them.

✅ If you want, I can also explain **something most drivers don't realize:**

- how police or manufacturers can sometimes **extract hidden pre-crash video buffers**, and
- which brands actually **store the most camera footage**.

NEXT NEW ChatGPT QUERY

ChatGPT query= "How do police or manufacturers sometimes extract hidden pre-crash video buffers, and which brands actually store the most camera footage

Get responses tailored to you

Log in to get answers based on saved chats, plus create images and upload files.

• How do police or manufacturers sometimes extract hidden pre-crash video buffers, and which brands actually store the most camera footage

Police and forensic investigators can sometimes recover **hidden "pre-crash" video buffers** from modern vehicles because many cars continuously record short loops of camera footage and telemetry in the

background. Even when the driver never saved the clip, fragments may still exist in memory, storage devices, or manufacturer systems. Here's how it usually works.

---

1. How "pre-crash buffers" actually work

Many modern cars record **continuous loop video** from cameras used for ADAS or autonomy. Instead of saving everything, the system keeps only the **last few seconds or minutes** in a temporary buffer.

When something triggers an event (airbag deployment, collision sensor, driver pressing save):

- The system copies the **previous buffer + some time after the event** into permanent storage.
- Older video is overwritten if nothing happens.

Example systems:

- **Tesla dashcam** saves **~10 minutes before a crash** if the feature is enabled.

BMW Drive Recorder saves about **20 seconds before and after an incident**.

Subaru EyeSight stores roughly **22 seconds around the crash**.

Separately, most vehicles have an **Event Data Recorder (EDR)** ("black box") that logs **vehicle dynamics for ~30 seconds** before a crash, such as speed, braking, and seatbelt status.

---

2. How investigators recover hidden footage

Digital-forensics teams can sometimes extract video **even if the driver never saved it**.

1 Pulling storage devices

If the vehicle uses removable storage (USB/SD):

- Investigators clone the drive.
- They run **file-carving software** to recover overwritten or deleted video segments.

Typical tools used in vehicle forensics:

- EnCase
- FTK (Forensic Toolkit)
- Autopsy
- Photorec / file-carving tools

These can recover **partial MP4 fragments from loop buffers**.

---

2 Direct ECU / infotainment extraction

Cars store data in several modules:

- Infotainment system
- ADAS camera module
- Telematics unit
- Autonomy computer (e.g., Tesla FSD computer)

Forensic labs may:

- Remove the module
- Access memory chips
- Dump flash storage

This can recover:

- temporary ring-buffer video
- sensor data
- timestamps and GPS

3️⃣ Manufacturer forensic reports

Some companies provide **official crash data reports**.

For example:

- Tesla vehicle data reports
- GM OnStar crash telemetry
- fleet telematics systems

These sometimes include:

- speed and braking
- driver inputs
- limited camera data

(Some require a subpoena or owner consent.)

4️⃣ Cloud or app data

Modern vehicles also sync with mobile apps or servers.

Investigators may obtain:

- trip history
- parking locations
- vehicle unlock events
- telematics logs

Forensic research has shown that **vehicle apps can reconstruct trips and driver actions** even when the car itself is unavailable.

---

3. Brands that store the MOST camera footage

Not all manufacturers store much video. The leaders are typically those designed around camera systems.

Tesla
Most extensive recording system.

Capabilities:

- Multiple cameras (front, rear, side)
- Dashcam recording while driving
- **Sentry Mode recording while parked**
- Up to **~10 minutes pre-event footage saved**.

Because the cameras run continuously for autonomy, Tesla vehicles often produce **the richest forensic video evidence**.

BMW
Drive Recorder uses surround cameras.

Features:

- 4-camera surround view recording
- ~20–30 seconds before and after events
- optional longer recording modes in some models.

Mercedes-Benz
Built-in dashcam in many models.

Characteristics:

- front camera recording
- loop recording to USB
- speed and location metadata.

Other brands with smaller buffers
Some cars record limited crash footage:

- Toyota (integrated dashcam accessory)

- Lexus
- Subaru (EyeSight ~22 seconds)
- Hyundai / Cadillac optional systems.

These systems typically store **far less footage** than Tesla or BMW.

---

4. Why hidden buffers sometimes survive

Even when footage appears gone, it may still exist because:

- Loop recordings **overwrite slowly**
- Files are only "deleted" in the index
- Flash storage keeps fragments
- Crash interruptions prevent overwrite completion

So investigators can sometimes recover **partial clips from seconds before impact**.

✅ **Summary**

Police and forensic analysts recover pre-crash footage by:

- extracting USB/SD storage
- cloning infotainment or camera modules
- recovering deleted loop-buffer files
- obtaining manufacturer crash reports
- analyzing vehicle apps or telematics

Brands with the most stored footage:

These usually record **telemetry, not video** in the Event Data Recorder (EDR).

Typical retention examples:

Manufacturer	Non-crash buffer
GM	~7–10 days telemetry
Ford	~3–5 days telemetry
Toyota/Lexus	~24–48 hours telemetry

But this data is **vehicle dynamics**, not camera footage.

Why Some Cars Keep 30–60+ Minutes

Cars with ADAS/self-driving systems already run multiple cameras.
Keeping a **long circular video buffer** allows them to:

- reconstruct accidents
- train autonomous driving systems
- capture vandalism or theft
- support insurance disputes

Vehicles that have cabin cameras / interior recording

These are usually for **driver monitoring or ADAS/autonomy systems**.

Brands that currently include interior cameras

These are the most common ones.

- **Tesla**
- **General Motors** (Cadillac Super Cruise)
- **Ford** (BlueCruise models)
- **Subaru** (DriverFocus)
- **BMW**
- **Mercedes-Benz**
- **Toyota** (some Lexus/Toyota driver monitoring)
- **Hyundai** / **Kia**

Examples with interior cameras:

- **Tesla Model 3**
- **Tesla Model Y**
- **Cadillac Escalade** (Super Cruise driver monitoring camera)

Subaru Forester (DriverFocus facial recognition)

What they actually do:

- Track **eyes, head position, attentiveness**
- Prevent misuse of driver-assist systems
- Some store **short clips or snapshots**

Most manufacturers say these cameras **process data locally and don't upload video** unless an event occurs or data sharing is enabled.

Sources

-

  CarExpert

  Dashcams: Which cars have them built-in? | CarExpert

  October 22, 2022

  Auto Express Car

  Built-In Dashcams: What You Need to Know - Auto Express Car

  March 10, 2025

  Car Buyer Labs

  Recording the Road Ahead: What Brands Have Built-in Dash Cams?

December 22, 2024

Tesla

Model Y Owner's Manual | Tesla

arXiv

Grand Theft App: Digital Forensics of Vehicle Assistant Apps

Kevin's Autos

Do any new cars come with a built-in dash cam?

June 11, 2025

More

-

visionarylawgroup.com

Black Box Car Accident Evidence: EDR Data That Strengthens Your Claim – Visionary Law Group

December 22, 2025 — See general prevalence and location notes in this EDR overview. * Short data window. Most EDRs store only 5–20 seconds of pre/post-crash data and 1–3 events total; overwriting is possible if the car i...

figliotech.com

Which Cars Have Built-In Dash Cams? The 2024-2025 Factory Integrated Guide - Dec 20, 2025

December 19, 2025 — December 20, 2025 WHICH CARS HAVE BUILT-IN DASH CAMS? THE 2024-2025 FACTORY INTEGRATED GUIDE DO ANY CARS HAVE BUILT

IN DASH CAMERAS? A 2025 GUIDE TO INTEGRATED RECORDING If you are wondering, 'do a...

cardashboardcameras.com

How Does Dash Cam Emergency Recording Work?

December 16, 2025 — Models equipped with Sony image sensors ensure that protected emergency recordings maintain superior video quality even during challenging lighting conditions when incidents occur. Similarly, buffered...

crimesdigest.com

D4vd Tesla Black Box Data: What A “Silent Witness” Could Reveal

September 26, 2025 — D4VD TESLA BLACK BOX DATA: WHAT A “SILENT WITNESS” COULD REVEAL IN THE CELESTE RIVAS INVESTIGATION by Christopher Winchell, Esq. 5 months ago written by Christopher Winchell, Esq. 5 months ago 0 co...

automedian.com

Which Cars Have Built In Dash Cam - Auto Median

September 9, 2025 — WHICH CARS HAVE BUILT IN DASH CAM by Chris Perling Disclosure This website is a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a mean...

tesla.com

Tesla's Integrated Vehicle Dashcam Adds a Layer of Security for Drivers | Tesla

March 31, 2025 — TESLA'S INTEGRATED VEHICLE DASHCAM ADDS A LAYER OF SECURITY FOR DRIVERS April 1, 2025 Dash cameras have become indispensable tools for modern drivers, offering a layer of security, convenience and p...

kbb.com

Car Event Data Recorder: The Black Box That Saves Money - Kelley Blue Book

March 4, 2024 — CAR EVENT DATA RECORDER: THE BLACK BOX THAT SAVES MONEY By Image Renee Valdes 03/05/2024 8:00am Image: Customer meeting with insurance agent after accident. EDR can provide details. QUICK FACTS AB...

dashcamdiscount.com

6 Car Brands With An In-Built Dashcam – Dash Cam Discount

October 13, 2023 — 6 CAR BRANDS WITH AN IN-BUILT DASHCAM Image: Photo of author Zach Harmon Updated: October 14, 2023 Dash cams have been a popular aftermarket addition for drivers due to their safety benefits. One...

eyewitnessdashcams.com

7 Car Brands with Built-In Dash Cams - Eyewitness Dashcams

August 17, 2020 — CADILLAC ImageImage This is for 2016 to 2019 Cadillac CT6 models only. I've scoured their websites and I think they have have discontinued them in future models. Anyways, the CT6 utilized 4 exterior...

washingtonpost.com

My Tesla was in a hit and run. It recorded the whole thing. - The Washington Post

February 26, 2020 — MY CAR WAS IN A HIT-AND-RUN. THEN I LEARNED IT RECORDED THE WHOLE THING. The car is becoming a sentry, a chaperone, and a snitch February 27, 2020 More than 5 years ago Make us preferred on Google...

cyrrup.com

Event Data Recorder (EDR) - Records & Helps investigate Accidents

November 7, 2017 — This reduces the threat to data-ownership or any lack of clarity on it. BEST SOLUTION WITH THE BEST PROTECTION Cyrrup's Camera Fleet solutions come with features that make the data accurate as well...

boxinformed.blogspot.com

Event Data Recorder - Black Box Video Camera - Box Information Center

August 21, 2015 — EVENT DATA RECORDER - BLACK BOX VIDEO CAMERA By AmiBox - 00.03 (2015-08-22T00:03:00-07:00) An event data recorder or EDR is a device installed in some automobiles to record information related to v...

policemag.com

In-car Video: Eyes on the Road | Police Magazine

October 27, 2014 — Features include: an internal hard drive that can hold up to 1,100 hours of data; built-in GPS; eight independent alarm inputs for triggering cameras; touchscreen controls for manual record, zoom, and...

roadproof.com

Traffic Camera Footage After Your Car Accident | Road Proof

FIND YOUR VIDEO. Click to download. Or we'll find it for you. Get instant access to millions of hours of recorded video & weather data from thousands of traffic cameras across the U.S. Get Started...

carmalegal.com

What You Need To Know About Black Box Data In Accidents | Carma Legal

Unlike aircraft recorders, a car's EDR does not capture audio. Its primary function is to detect crash events and deploy safety systems like airbags, then

record crucial crash data as a secondary feat...

E

sciencedirect.com

Analysis of real-time operating systems' file systems: Built-in cameras from vehicles - ScienceDirect

3. EXPERIMENTAL ENVIRONMENT (DVRS) The HYUNDAI/KIA/GENESIS launched with built-in DVRS installed on and over 34 such models are released since 2019 (Hyundai, 2022a, Hyundai, 2022b). The DVRS can reco...

nhtsa.gov

Event Data Recorder | NHTSA

2003 Agent, K. R.; Pigman, J. G.; Barrett, M. L.; Green, E. R. 2003. Analysis of traffic crash data in Kentucky (1998-2002) Kentucky University , Lexington , Kentucky Transportation Center. 139 p. Re...

crashforensics.com

Automobile Crash Event Data Recorder Downloading

However, some do store pre-crash data including Vehicle Speed Sensor (VSS) data for a period of five to twenty seconds before an impact. Image What Vehicles Have This EDR Function? ImageIt is reasonab...

CI

crenshawinvestigations.com

Event Data Recorder Extraction | Crenshaw Investigations

(213) 373-4833 Robert@CrenshawInvestigations.com EVENT DATA RECORDER EXTRACTION | CRENSHAW INVESTIGATIONS EVENT DATA RECORDER EXTRACTION Crenshaw Investigations specializes in Event Data Recorder...

NEXT NEW ChatGPT QUERY

ChatGPT query= "The multiple hidden cameras and microphones secreted in modern cars are often unknown to the owner. Who gets to watch and

listen to these recordings, how long are they retained, and does the car stop working if they are disabled."

The issue of surveillance in modern cars, particularly with regards to hidden cameras and microphones, raises significant concerns about privacy, security, and data usage. Here's a breakdown of the key points you raised:

1. Who gets to watch and listen to these recordings?

- **Car Manufacturers:** Many modern vehicles are equipped with cameras and microphones for features like driver assistance (e.g., lane-keeping, collision avoidance), infotainment, voice control, and autonomous driving. Car manufacturers may have access to this data, especially if it's used for improving the system's performance or for software updates. Some data could potentially be shared with third parties, such as insurance companies (in case of accidents) or service providers.

- **Remote Surveillance:** Some high-end vehicles offer features like "driver monitoring" or "sentiment detection," which could involve the collection of data. In certain scenarios, manufacturers could have the ability to remotely monitor the vehicle. However, data collection is usually anonymized, but the potential for misuse exists.

- **Third Parties:** In some cases, third parties may also access vehicle data for various purposes, including law enforcement agencies with proper legal authorization, or potentially data brokers for targeted advertising (although this is more of an emerging concern in the context of smart devices).

2. How long is the data retained?

- **Data Retention Policies:** Typically, manufacturers and service providers outline how long data is retained in their terms and conditions. Some data (like GPS logs or audio recordings) might be stored temporarily to improve service performance or provide safety features, but it could be deleted after a certain period. However, there is no standard across the industry, and policies can vary widely.

- **Vehicle Data Management:** In some cars, especially those with self-driving capabilities, data is stored locally on the vehicle or in cloud servers for analysis and software updates. The duration depends on the purpose, but in some cases, data might be retained indefinitely until it is manually deleted by the owner or overridden by new data.

3. Does the car stop working if surveillance systems are disabled?

- **Disabling Systems:** It's unlikely that the entire car would stop functioning if you disabled the cameras and microphones, but it may affect certain features. For instance, driver-assist systems, autonomous driving functions, and parking aids often rely on cameras and sensors to work properly. If these systems are disabled, features like adaptive cruise control, automatic emergency braking, or lane-keeping assist might not function as expected.

- **Legality and Warranty Considerations:** Disabling certain surveillance or safety systems might void the vehicle's warranty or could be illegal in some jurisdictions, especially if they are critical for safety. It's important to review your car's owner manual and the terms of the warranty before making changes to such systems.

4. Is any of the data RF transmitted?

- **RF Transmission:** Some vehicle data may be transmitted via radio frequency (RF) signals, particularly in the case of telematics systems that send data about the car's location, diagnostics, and performance to a central server. This is often done through cellular networks (e.g., 4G/5G) or Wi-Fi. However, specific recordings from cameras and microphones are typically stored locally or uploaded when the vehicle connects to a network.

- **Connected Cars and Data Privacy Concerns:** Modern "connected cars" often have the capability to transmit data over RF, such as GPS location, driving habits, and other telemetry. However, whether or not sensitive data (like audio or video

recordings) is transmitted through RF is dependent on the vehicle's specific systems. Most systems are designed to transmit only necessary data for things like navigation or emergency services.

Final Thoughts:

While the increasing use of cameras, microphones, and data collection in cars is useful for safety and convenience, it does raise important concerns regarding privacy, consent, and data management. It's crucial for car owners to understand the extent of surveillance in their vehicle, review manufacturer policies regarding data collection and retention, and ensure that any changes to these systems do not violate warranties or local regulations.

If you're concerned about these issues, consider consulting with your car's manufacturer or a legal expert for more tailored advice.

NEXT NEW ChatGPT QUERY

ChatGPT query= “What kind of legal protection in the USA exists for privacy, admissibility, or civil damages when harm is done with audio or video data that is secretly gathered and abused?”

The issue of surveillance in modern cars, particularly with regards to hidden cameras and microphones, raises significant concerns about privacy, security, and data usage. Here's a breakdown of the key points you raised:

1. Who gets to watch and listen to these recordings?

- **Car Manufacturers:** Many modern vehicles are equipped with cameras and microphones for features like driver assistance (e.g., lane-keeping, collision avoidance), infotainment, voice control, and autonomous driving. Car manufacturers may have access to this data, especially if it's used for improving the system's performance or for software updates. Some data could potentially be shared with third parties, such as insurance companies (in case of accidents) or service providers.

- **Remote Surveillance:** Some high-end vehicles offer features like "driver monitoring" or "sentiment detection," which could involve the collection of data. In certain scenarios, manufacturers could have the ability to remotely monitor the vehicle. However, data collection is usually anonymized, but the potential for misuse exists.
- **Third Parties:** In some cases, third parties may also access vehicle data for various purposes, including law enforcement agencies with proper legal authorization, or potentially data brokers for targeted advertising (although this is more of an emerging concern in the context of smart devices).

2. How long is the data retained?

- **Data Retention Policies:** Typically, manufacturers and service providers outline how long data is retained in their terms and conditions. Some data (like GPS logs or audio recordings) might be stored temporarily to improve service performance or provide safety features, but it could be deleted after a certain period. However, there is no standard across the industry, and policies can vary widely.
- **Vehicle Data Management:** In some cars, especially those with self-driving capabilities, data is stored locally on the vehicle or in cloud servers for analysis and software updates. The duration depends on the purpose, but in some cases, data might be retained indefinitely until it is manually deleted by the owner or overridden by new data.

3. Does the car stop working if surveillance systems are disabled?

- **Disabling Systems:** It's unlikely that the entire car would stop functioning if you disabled the cameras and microphones, but it may affect certain features. For instance, driver-assist systems, autonomous driving functions, and parking aids often rely on cameras and sensors to work properly. If these systems are disabled, features like adaptive cruise control, automatic emergency braking, or lane-keeping assist might not function as expected.

- **Legality and Warranty Considerations:** Disabling certain surveillance or safety systems might void the vehicle's warranty or could be illegal in some jurisdictions, especially if they are critical for safety. It's important to review your car's owner manual and the terms of the warranty before making changes to such systems.

4. Is any of the data RF transmitted?

- **RF Transmission:** Some vehicle data may be transmitted via radio frequency (RF) signals, particularly in the case of telematics systems that send data about the car's location, diagnostics, and performance to a central server. This is often done through cellular networks (e.g., 4G/5G) or Wi-Fi. However, specific recordings from cameras and microphones are typically stored locally or uploaded when the vehicle connects to a network.

- **Connected Cars and Data Privacy Concerns:** Modern "connected cars" often have the capability to transmit data over RF, such as GPS location, driving habits, and other telemetry. However, whether or not sensitive data (like audio or video recordings) is transmitted through RF is dependent on the vehicle's specific systems. Most systems are designed to transmit only necessary data for things like navigation or emergency services.

Final Thoughts:

While the increasing use of cameras, microphones, and data collection in cars is useful for safety and convenience, it does raise important concerns regarding privacy, consent, and data management. It's crucial for car owners to understand the extent of surveillance in their vehicle, review manufacturer policies regarding data collection and retention, and ensure that any changes to these systems do not violate warranties or local regulations.

If you're concerned about these issues, consider consulting with your car's manufacturer or a legal expert for more tailored advice.

NEXT NEW ChatGPT QUERY

ChatGPT query="What kind of legal protection in the USA exists for privacy, admissibility, or civil damages when harm is done with audio or video data that is secretly gathered and abused?"

In the U.S., privacy laws related to secretly gathered audio and video data—especially in the context of harm caused by misuse—are complex and often involve multiple layers of legal protections and challenges. These laws primarily deal with issues of consent, admissibility of evidence, and the potential for civil damages. Here's an overview of the key protections that may be relevant:

1. Consent Laws and Privacy Expectations

- **Federal Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968):**
    - **Key Provisions:** The Wiretap Act prohibits the intentional interception or disclosure of wire, oral, or electronic communications without the consent of at least one party involved.
    - **Application:** In the context of secret audio and video recordings, if someone secretly records conversations (for example, in a car) without consent, they could be violating the Wiretap Act, assuming that the communication involves "oral" conversations. However, the law primarily applies to communications that are "intercepted" in transit rather than stored data.
    - **Exceptions:** The law allows for certain exceptions, such as when law enforcement is involved, or if one party consents to the recording. Some states also allow "one-party consent" for audio recordings, meaning if one person

involved in the conversation consents, the recording can be made legally.

- **State-Specific Laws:**
    - Each state may have its own laws about consent for audio and video recordings. Some states follow **one-party consent** rules, while others require **all-party consent** (i.e., everyone involved in the conversation must agree to be recorded). For example, California has an all-party consent rule, meaning that both the driver and any passengers in the car would need to be informed and give consent for any audio or video recordings.
    - Violating these laws can lead to criminal charges and civil liabilities.
- **Expectation of Privacy (Fourth Amendment):**
    - **Key Principle:** The Fourth Amendment of the U.S. Constitution protects against unreasonable searches and seizures by the government. This applies to personal privacy, including electronic communications. The expectation of privacy plays a critical role in whether secret audio/video recordings are deemed unlawful.
    - **Application to Vehicles:** Generally, there is an expectation of privacy inside a private vehicle. Unauthorized surveillance—especially audio recordings of conversations—could be seen as violating that expectation of privacy. However, if someone knowingly uses a product that involves surveillance (e.g., smart cars or certain apps), their expectation of privacy may be reduced.

2. Admissibility of Audio/Video Evidence

- **Federal Rules of Evidence:**
    - In legal proceedings, the **admissibility of secretly recorded audio or video** depends on whether the recording was made in compliance with relevant laws. If

the recording violates state or federal wiretapping laws (e.g., no consent), it may be inadmissible in court.

- **Hearsay Rules:** Audio or video recordings may also be subject to hearsay rules if the recording is used to prove the truth of the matter asserted (e.g., in criminal or civil cases). There are exceptions, but if the recording was made unlawfully, this could complicate its admissibility.

- **Exclusionary Rule (Fruit of the Poisonous Tree):**
  - Under this principle, evidence obtained through illegal means may be excluded from court. So, if an audio or video recording was made secretly and unlawfully, it could potentially be excluded as evidence in a trial, including criminal trials or civil litigation.

3. Civil Damages for Privacy Violations

- **Civil Suits Under the Wiretap Act:**
  - Individuals harmed by illegal wiretapping or secret recordings can file a civil lawsuit under the **Federal Wiretap Act**. If successful, the victim can recover damages, which may include:
    - **Actual damages** (actual harm suffered due to the violation).
    - **Statutory damages**, which can range from $100 to $500 per violation, even if the victim cannot prove actual harm.
    - **Punitive damages** (to punish the wrongdoer for egregious conduct) may also be awarded in some cases.
  - **State Laws:** Many states also allow victims to sue for damages if their privacy was violated by illegal recordings. For example, California's **Invasion of Privacy Act** gives

individuals the right to sue for damages when their private conversations are illegally recorded.

- **Defamation and Emotional Distress Claims:**
    - In addition to privacy laws, a person harmed by the misuse of secretly obtained audio/video data could also bring a civil suit for defamation (if the recordings are used to damage their reputation) or **intentional infliction of emotional distress** if the release or use of such recordings caused significant psychological harm.
- **Breach of Contract (Consumer Protection):**
    - If the audio or video data was obtained via an agreement with a company (such as a car manufacturer, app provider, or service), the misuse of that data may result in a **breach of contract** claim. For example, if a manufacturer secretly gathers data and misuses it in violation of privacy policies, affected consumers could potentially seek damages.

4. Additional Legal Protections

- **FTC Regulations:** The **Federal Trade Commission (FTC)** enforces privacy laws related to consumer protection. If a company secretly collects and abuses consumer data (e.g., violating privacy policies or terms of service), the FTC can investigate and impose penalties for unfair or deceptive practices.
- **Data Breach Laws:** If private audio/video data is mishandled, exposed, or unlawfully accessed (e.g., due to poor security practices), individuals may have the right to seek damages under data breach laws, such as those found in the **California Consumer Privacy Act (CCPA)** and similar state-level privacy laws.
- **Privacy Torts:** In some instances, individuals may sue for the **tort of intrusion upon seclusion** if their private conversations

or activities were secretly recorded without consent and used against them in harmful ways.

Summary:

In the U.S., there are several legal protections against the secret gathering and abuse of audio and video data:

- **Federal and state wiretap laws** govern the recording of conversations, requiring consent and imposing criminal and civil penalties for violations.
- **The Fourth Amendment** provides privacy protections, especially in private spaces like vehicles, which could limit the use of secret recordings by third parties.
- **Civil damages** are available under the **Wiretap Act**, state privacy laws, or as part of a **tort claim** (such as defamation or emotional distress).
- **Admissibility** of secretly gathered audio/video evidence is limited in court if it violates privacy laws.

Victims of such harm may be able to file lawsuits for both damages and injunctive relief to stop the abuse. However, the exact remedies depend on the circumstances and the specific legal violations involved.

Conclusion

Privacy laws concerning secretly made audio or video recordings in the U.S. are complex and vary depending on federal and state laws, as well as constitutional protections. In general, recording without consent is subject to limitations based on whether the recording is taking place in a public or private setting, the purpose of the recording, and whether one or both parties consent. The ACLU plays an important role in defending individuals' rights related to these recordings, particularly in cases involving free speech, public interest, and constitutional privacy protections.

How believable are the providers of Surveillance Capitalism?

Harvard professor Shoshana Zuboff wrote a monumental book about the new economic order that is alarming. "The Age of Surveillance Capitalism," and is featured in a free VPRO documentary "On Surveillance Capitalism," reveals how the biggest tech companies deal with our data. How do we regain control of our data? What is surveillance capitalism? In this documentary, Zuboff takes the lid off Google and Facebook and reveals a merciless form of capitalism in which no natural resources, but the citizen itself, serves as a raw material. How can citizens regain control of their data? It is 2000, and the dot.com crisis has caused deep wounds. How will startup Google survive the bursting of the internet bubble? Founders Larry Page and Sergey Brin don't know anymore how to turn the tide. By chance, Google discovers that the "residual data" that people leave behind in their searches on the internet is very precious and tradable. This residual data can be used to predict the behavior of the internet user. Internet advertisements can, therefore, be used in a very targeted and effective way. A completely new business model is born: "surveillance capitalism."

While industrial capitalism exploited and controlled nature with devastating consequences, surveillance capitalism exploits and controls human nature with a totalitarian order as the endpoint of the development. Google was fined several billion dollars by the EU because it had abused its monopoly position in Europe.

Premise

Zuboff states that surveillance capitalism "unilaterally claims human experience as free raw material for translation into behavioural data [which] are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into *prediction products* that anticipate what you will do now, soon, and later." She states that these new capitalist

products "are traded in a new kind of marketplace that I call *behavioural futures markets*."

In a capitalist society, information, such as a user's likes and dislikes gathered when accessing a platform like Facebook, or from any other kind of sensor that serves as an internet touch point to data-stream, is information that can be used by that company to better the experience of a user by feeding them information that data obtained from their previous activity would have shown them to be interested in. It can also infer many things about the individual that extend far beyond the terms and conditions of use.

This in many ways can be done through the use of an algorithm that analyses information. The danger of surveillance capitalism is that platforms and tech companies claim ownership of private information because it is free for them to access, claiming private experience as 'raw material' for data factories. There is very little supervision or actual laws by governments and users themselves. Because of this, there has been backlash on how these companies have used the information gathered. For example, Google, which is said to be "the pioneer of surveillance capitalism"] introduced a feature that used "commercial models … discovered by people in a time and place" This means that not only are commercials being specifically targeted to you through your phone, but now work hand in hand with your environment and habits such as being shown an advertisement of a local bar when walking around downtown in the evening. Advertising attempts this technical and specific can easily have an impact on the one's decision-making process in the activities they choose and in political decisions. Thus the idea that these companies seemingly go unchecked whilst having the power to observe and control thinking is one of the many reasons tech companies such as Google themselves are under so much scrutiny and criticism.

Furthermore, Zuboff writes, the freedom allotted to tech companies comes from the idea that "surveillance capitalism does not abandon

established capitalist 'laws' such as competitive production, profit maximization, productivity and growth", as they are principles any business in a capitalistic society should aim to excel in, in order to be competitive. Zuboff claims in an article that "new logic accumulation … introduces its own laws of motion". In other words, this is a new phenomenon in capitalistic operations that should be treated as such and be instilled with its own specific restrictions and limitations. Lastly, as invasive as platforms have been in terms of accumulating information, they have also led to what is now called a "sharing economy", Van Dijck (2018) in which digital information can be obtained by individuals carrying out their own surveillance capitalism through the aid of platforms themselves. Thus "individuals can greatly benefit from this transformation because it empowers them to set up business", Van Dijck (2018). Small businesses will also benefit in potentially growing faster than they would have without knowing consumer demands and wants but would need to pay corporations for access to knowledge. This leaves surveillance capitalism as an exceptionally useful tool for businesses, but also an invasion of privacy to users who do not want their private experience to be owned by a company.

*Our ignorance is their bliss.*They place hidden microphones and cameras in products to monitor its customers and secretly profile them. This massive database allows them to make generalizations that can be broadly applied to human behavior.

What is not discussed are the political consequences, how technocrat billionaires band together to create narratives and public expectations in advance regarding technologies they would like to be embraced but unregulated, like AI, quantum computing, cool fusion clean nuclear power, antigravity technology, cryptocurrencies, etc. They have lots of money to spend, back room corporate goals and clearly documented service-to-self motives to get things in their pocket before a legal framework is established protecting the public good.

The out of sight, out of mind, profits first regardless of legal consequences outlook efforts to control the planet are disclosed here, politely called by names like obfuscation and denial. Morality is at a minimum, reassurances are tokenisms, but where is life, liberty and the pursuit of happiness with a loving and open heart? How do you implement trust, beauty, and fair play for all in a world dominated by price tags? New legal ground is fertile for any disruption to society technocrats choose to make. The debates come later when their behavior is challenged in court. They got there first and made their own rules. What's a few billion dollars in fines when trillions are at stake?

They get to create new tools that businesses and politicians can use as they please. All their data is for sale to those with pockets deep enough to pay the price and they collect that data when ever and how ever it suits them. That's the way of creative corporate capitalists!

The movie *2000 Mules* gives the public a clear idea just how available public cell phone location data is for those with deep pockets like Google.

Technocratic billionaires are rich and notorious. They would be happy to rule the world with their brand of technical globalism. Do we want to end up like the Uighurs in China who are imprisoned by their Chinese providers brand of surveillance? No cells or bars are needed, technology does the trick very economically.